kaspersky

Kaspersky SIEM Cloud

© 2026 АО "Лаборатория Касперского"

Содержание

- Kaspersky SIEM Cloud
  - О решении
  - Архитектура решения
  - Аппаратные и программные требования
    - Требования к устройствам Windows для установки агентов
    - Требования к устройствам Linux для установки агентов
    - Требования к устройствам с операционными системами Oracle Linux, Astra Linux, Ubuntu, РЕД ОС, Мос ОС
    - Требования для локальных компонентов
  - Совместимые приложения и решения
  - Настройка исключений в Kaspersky Endpoint Security для Linux
  - О предоставлении данных
- Начало работы
  - Интерфейс Консоли OSMP
    - Изменение домашней страницы OSMP Console
    - Изменение языка интерфейса и темы
    - Добавление и удаление закладок
    - Возврат к списку рабочих областей
  - Активация и первоначальная настройка Kaspersky SIEM Cloud
  - Типовая конфигурация решения
  - Проверка настройки Kaspersky SIEM Cloud
  - Деактивация Kaspersky SIEM Cloud
- Администрирование с помощью Kaspersky Security Center Cloud Console
  - Руководство по усилению защиты
    - Планирование архитектуры Kaspersky Security Center Cloud Console
    - Учетные записи и авторизация
    - Управление защитой клиентских устройств
    - Настройка защиты управляемых приложений
    - Передача событий в сторонние системы
    - Рекомендации по безопасности сторонних информационных систем
    - Рекомендации по использованию приложений безопасности "Лаборатории Касперского"
  - Сценарий: создание иерархии Серверов администрирования, управляемых с помощью Kaspersky Security Center Cloud Console
  - Перенос данных в Kaspersky Security Center Cloud Console
    - Способы переноса данных в Kaspersky Security Center Cloud Console
    - Сценарий: перенос данных без иерархии Серверов администрирования
    - Мастер переноса данных
      - Шаг 1. Экспорт управляемых устройств, объектов и параметров из Kaspersky Security Center Web Console
      - Шаг 2. Импорт файла экспорта в Kaspersky Security Center Cloud Console
      - Шаг 3. Переустановка Агента администрирования на управляемых устройствах с помощью Kaspersky Security Center Cloud Console
    - Перенос данных с иерархией Серверов администрирования
    - Сценарий: перенос данных устройств с операционными системами Linux или macOS
    - Сценарий: обратный перенос данных из Kaspersky Security Center Cloud Console в Kaspersky Security Center

- Перенос данных с виртуальными Серверами администрирования
  - Сценарий: перенос данных с виртуальными Серверами администрирования с помощью перемещения устройств
  - Сценарий: перенос данных с виртуальными Серверами администрирования вручную
  - Сценарий: перемещение устройств из групп администрирования под управление виртуальных Серверов
- Выбор региона для доступа к Kaspersky Security Center Cloud Console
- Мастер первоначальной настройки
  - О мастере первоначальной настройки
  - Запуск мастера первоначальной настройки
  - Шаг 1. Выбор инсталляционных пакетов для загрузки
  - Шаг 2. Настройка параметров прокси-сервера
  - Шаг 3. Настройка Kaspersky Security Network
  - Шаг 4. Настройка управления обновлениями приложений сторонних производителей
  - Шаг 5. Создание базовой конфигурации защиты сети
  - Шаг 6. Завершение работы мастера первоначальной настройки
- Первоначальное развертывание приложений "Лаборатории Касперского"
  - Сценарий: первоначальное развертывание приложений "Лаборатории Касперского"
  - Создание инсталляционных пакетов для приложений "Лаборатории Касперского"
  - Распространение инсталляционных пакетов на подчиненные Серверы администрирования
  - Создание автономных инсталляционных пакетов Агента администрирования
  - Просмотр списка автономных инсталляционных пакетов
  - Создание пользовательского инсталляционного пакета
  - Требования для точки распространения
  - Параметры инсталляционного пакета Агента администрирования
  - Виртуальная инфраструктура
    - Рекомендации по снижению нагрузки на виртуальные машины
    - Поддержка динамических виртуальных машин
    - Поддержка копирования виртуальных машин
  - Использование Агента администрирования для Windows, Linux и macOS: сравнение
  - Указание параметров удаленной установки на устройствах под управлением Unix
  - Замещение приложений безопасности сторонних производителей
  - Возможности ручной установки приложений
  - Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky SIEM Cloud
  - Мастер развертывания защиты
    - Шаг 1. Запуск мастера развертывания защиты
    - Шаг 2. Выбор инсталляционного пакета
    - Шаг 3. Выбор версии Агента администрирования
    - Шаг 4. Выбор устройств
    - Шаг 5. Задание параметров задачи удаленной установки
    - Шаг 6. Управление перезагрузкой
    - Шаг 7. Удаление несовместимых приложений перед установкой
    - Шаг 8. Перемещение устройств в папку Управляемые устройства
    - Шаг 9. Выбор учетных записей для доступа к устройствам
    - Шаг 10. Запуск установки
  - Сетевые параметры для взаимодействия с внешними сервисами
  - Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования

Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux
Установка приложений с помощью задачи удаленной установки
Удаленная установка приложений
Установка приложений на подчиненные Серверы администрирования
Запуск и остановка приложений "Лаборатории Касперского"
Обнаружение сетевых устройств и создание групп администрирования
Сценарий: обнаружение сетевых устройств
Опрос сети
Опрос сети Windows
Опрос контроллеров домена
Опрос IP-диапазонов
Настройка контроллеров домена Samba
Добавление и изменение IP-диапазона
Настройка точек распространения и шлюзов соединений
Расчет количества и конфигурации точек распространения
Типовая конфигурация точек распространения: один офис
Типовая конфигурация точек распространения: множество небольших удаленных офисов
Назначение точек распространения вручную
Изменение списка точек распространения для группы администрирования
Использование точки распространения в качестве извещающего сервера
Использование параметра "Не разрывать соединение с Сервером администрирования" для обеспечения постоянной связи между управляемым устройством и Сервером администрирования
Создание групп администрирования
Создание правил перемещения устройств
Копирование правил перемещения устройств
Условия для правила перемещения устройств
Добавление устройств в состав группы администрирования вручную
Перемещение устройств или кластеров в состав группы администрирования вручную
Настройка правил хранения для нераспределенных устройств
Инвентаризация оборудования
Добавление информации о новых устройствах
Настройка критериев определения корпоративных устройств
Настройка приложений "Лаборатории Касперского"
Сценарий: настройка защиты сети
Подходы к управлению безопасностью, ориентированные на устройства и на пользователей
Настройка и распространение политик: подход, ориентированный на устройства
Настройка и распространение политик: подход, ориентированный на пользователя
Параметры политики Агента администрирования
Сравнение параметров политики Агента администрирования по операционным системам
Настройка параметров защиты управляемых приложений
Ручная настройка групповой задачи обновления Kaspersky Endpoint Security
Управление задачами
О задачах
Область задачи
Создание задачи
Просмотр списка задач

Запуск задачи вручную
Запуск задачи для выбранных устройств.
Общие параметры и свойства задач
Экспорт задачи
Импорт задачи
Просмотр результатов выполнения задач, хранящихся на Сервере администрирования
Управление клиентскими устройствами
Параметры управляемого устройства
Проверка соединения клиентского устройства с Сервером администрирования вручную Утилита klnagchk
Выборки устройств
Просмотр списка устройств из выборки устройств
Создание выборки устройств
Настройка выборки устройств
Экспорт списка устройств из выборки устройств
Удаление устройств из групп администрирования в выборке
Просмотр и настройка действий, когда устройство неактивно
О статусах устройства
Настройка переключения статусов устройств
Смена Сервера администрирования для клиентских устройств
Избегание конфликтов между Серверами администрирования
Создание профилей подключения к Серверу администрирования
О кластерах и массивах серверов
Свойства кластеров или массивов серверов
Теги устройств
Создание тегов устройств
Изменение тегов устройств
Удаление тегов устройств
Просмотр устройств, которым назначен тег
Просмотр тегов, назначенных устройству
Назначение тегов устройствам вручную
Снятие назначенных тегов с устройств
Просмотр правил автоматического назначения тегов устройствам
Изменение правил автоматического назначения тегов устройствам
Создание правил автоматического назначения тегов устройствам
Выполнение правил автоматического назначения тегов устройствам
Удаление правил автоматического назначения тегов с устройств
Управление тегами устройств с помощью утилиты klscflag
Карантин и Файлы резервного хранилища
Загрузка файла из хранилища
Удаление файлов из хранилища
Удаленная диагностика клиентских устройств
Открытие окна удаленной диагностики
Включение и выключение трассировки для приложений
Загрузка файла трассировки приложения
Удаление файлов трассировки
Загрузка параметров приложений
Загрузка системной информации с клиентского устройства

Загрузка журналов событий
Запуск, остановка и перезапуск приложения
Запуск удаленной диагностики приложения и загрузка результатов
Запуск приложения на клиентском устройстве
Создание файла дампа для приложения
Удаленное подключение к рабочему столу клиентского устройства
Подключение к устройствам с помощью совместного доступа к рабочему столу Windows
Срабатывание правил в режиме Интеллектуального обучения
Просмотр списка обнаружений, выполненных с помощью правил Адаптивного контроля аномалий
Добавление исключений в правила Адаптивного контроля аномалий
Управление группами администрирования
Создание групп администрирования
Автоматическая установка приложений на устройства группы администрирования
Перемещение групп администрирования
Удаление групп администрирования
Политики и профили политик
Блокировка (замок) и заблокированные параметры
Наследование политик и профилей политик
Иерархия политик
Профили политик в иерархии политик
Как параметры реализованы на управляемом устройстве
Управление политиками
Просмотр списка политик
Создание политики
Изменение политики
Общие параметры политик
Включение и выключение параметра наследования политики
Копирование политики
Перемещение политики
Экспорт политики
Импорт политики
Просмотр диаграммы состояния применения политики
Автоматическая активация политики по событию "Вирусная атака"
Принудительная синхронизация
Удаление политики
Управление профилями политик
Просмотр профилей политики
Изменение приоритета профиля политики
Создание профиля политики
Изменение профиля политики
Копирование профиля политики
Создание правила активации профиля политики
Удаление профиля политики
Экспорт и импорт профиля политики
Шифрование и защита данных
Просмотр списка зашифрованных жестких дисков
Формирование и просмотр отчетов о шифровании

Предоставление доступа к зашифрованному жесткому диску в автономном режиме
Передача ключей шифрования между Серверами администрирования
Управление пользователями и ролями пользователей
Об учетных записях пользователей
Добавление учетной записи внутреннего пользователя
Удаление учетной записи внутреннего пользователя
Назначение администраторов рабочей области
О ролях пользователей
Настройка прав доступа к функциям приложения. Управление доступом на основе ролей
Права доступа к функциям приложения
Предопределенные роли пользователей
Назначение прав доступа к набору объектов
Назначение прав пользователям или группам безопасности
Назначение роли пользователю или группе безопасности
Создание роли пользователя
Изменение роли пользователя
Изменение области для роли пользователя
Удаление роли пользователя
Связь профилей политики с ролями
Создание группы безопасности
Изменение группы безопасности
Добавление учетных записей пользователей во внутреннюю группу
Удаление группы безопасности
Настройка ADFS-интеграции
Настройка интеграции с Microsoft Entra ID
Включение опроса Microsoft Entra ID
Добавление Kaspersky Security Center Cloud Console в список приложений
Назначение пользователя владельцем устройства
Назначение пользователя владельцем устройства Linux после установки Агента администрирования
Работа с ревизиями объектов
Добавление описания ревизии
Откат изменений объекта к предыдущей ревизии
Просмотр и сохранение ревизии политики
Сравнение ревизий политики
Kaspersky Security Network (KSN)
О KSN
Включение и отключение KSN
Просмотр принятого Положения о KSN
Принятие обновленного Положения о KSN
Проверка, работает ли точка распространения как прокси-сервер KSN
Удаление объектов
Обновление баз и приложений "Лаборатории Касперского"
Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"
Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"
Создание задачи загрузки обновлений в хранилища точек распространения
Настройка управляемых устройств для получения обновлений только от точек распространения
Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky SIEM Cloud

Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows
О статусах обновлений
Одобрение и отклонение обновлений программного обеспечения
Использование файлов различий для обновления баз и модулей приложений "Лаборатории Касперского".
Обновление баз и модулей приложений "Лаборатории Касперского" на автономных устройствах
Управление сторонними приложениями и исполняемыми файлами на клиентских устройствах
Ограничения Системного администрирования
Доступность Системного администрирования в пробном и коммерческом режимах и при различных вариантах лицензирования
О приложениях сторонних производителей
Обновления приложений сторонних производителей
Сценарий: обновление приложений сторонних производителей
Установка обновлений приложений сторонних производителей
Создание задачи Поиск уязвимостей и требуемых обновлений
Параметры задачи поиска уязвимостей и требуемых обновлений
Создание задачи Установка требуемых обновлений и закрытие уязвимостей
Добавление правил для установки обновлений
Создание задачи Установка обновлений Центра обновления Windows
Просмотр информации о доступных обновлениях приложений сторонних производителей.
Экспорт списка доступных обновлений в файл
Одобрение и отклонение обновлений приложений сторонних производителей.
Автоматическое обновление приложений сторонних производителей
Обнаружение и закрытие уязвимостей в приложениях
Закрытие уязвимостей в приложениях
Создание задачи Закрытие уязвимостей
Создание задачи Установка требуемых обновлений и закрытие уязвимостей
Добавление правил для установки обновлений
Просмотр информации об уязвимостях в приложениях, обнаруженных на всех управляемых устройствах
Просмотр информации об уязвимостях в приложениях, обнаруженных на выбранных управляемых устройствах
Просмотр статистики уязвимостей на управляемых устройствах.
Экспорт списка уязвимостей в приложениях в текстовый файл
Игнорирование уязвимостей в приложениях
Сценарий: обнаружение и закрытие уязвимостей в приложениях
Установка максимального срока хранения информации о закрытых уязвимостях
Управление запуском приложений на клиентских устройствах
Использование компонента Контроль приложений для управления исполняемыми файлами
Режимы и категории компонента Контроль приложений
Получение и просмотр списка приложений, установленных на клиентских устройствах
Получение и просмотр списка исполняемых файлов, установленных на клиентских устройствах
Создание пополняемой вручную категории приложений
Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств
Просмотр списка категорий приложений
Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security for Windows
Добавление исполняемых файлов, связанных с событием, в категорию приложения
Создание инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"
Просмотр и изменение параметров инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"

Параметры инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"
Теги приложений
Создание тегов приложений
Изменение тегов приложений
Назначение тегов приложениям
Снятие назначенных тегов с приложений
Удаление тегов приложений
Настройка Сервера администрирования
Иерархия Серверов администрирования
Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования
Настройка срока хранения событий, относящихся к удаленным устройствам
Объединение электронной почты о событиях
Ограничения на управление подчиненными Серверами администрирования, работающими локально, с помощью Kaspersky Security Center Cloud Console
Просмотр списка подчиненных Серверов администрирования
Удаление иерархии Серверов администрирования
Настройка интерфейса
Управление виртуальными Серверами администрирования
Создание виртуального Сервера администрирования
Включение и выключение виртуального Сервера администрирования
Назначение администратора виртуального Сервера администрирования
Удаление виртуального Сервера администрирования
Удаленная диагностика клиентских устройств
Открытие окна удаленной диагностики
Включение и выключение трассировки для приложений
Загрузка файла трассировки приложения
Удаление файлов трассировки
Загрузка параметров приложений
Загрузка системной информации с клиентского устройства
Загрузка журналов событий
Запуск, остановка и перезапуск приложения
Запуск удаленной диагностики приложения и загрузка результатов
Запуск приложения на клиентском устройстве
Создание файла дампа для приложения
Запуск удаленной диагностики на клиентском устройстве с операционной системой Linux
Экспорт событий в SIEM-системы
Настройка экспорта событий в SIEM-системы
Предварительные условия
Об экспорте событий
Настройка экспорта событий в SIEM-системе
Выбор событий для экспорта в SIEM-системы в формате syslog
Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog
Выбор общих событий для экспорта в формате Syslog
Об экспорте событий в формате Syslog
Настройка Kaspersky SIEM Cloud для экспорта событий в SIEM-систему
Просмотр результатов экспорта

- Работа с Kaspersky Security Center Cloud Console в облачном окружении
  - Варианты лицензирования в облачном окружении
  - Подготовка к работе в облачном окружении с помощью Kaspersky Security Center Cloud Console
    - Работа в облачном окружении Amazon Web Services
      - О работе в облачном окружении Amazon Web Services
      - Создание учетных записей IAM-пользователя для инстансов Amazon EC2
        - Обеспечение прав для работы Kaspersky SIEM Cloud с AWS
        - Создание учетной записи IAM-пользователя для работы Kaspersky SIEM Cloud
    - Работа в облачном окружении Microsoft Azure
      - О работе в Microsoft Azure
      - Создание подписки, идентификатора приложения и пароля
      - Назначение роли для ID приложения в Azure
    - Работа в Google Cloud
  - Мастер настройки для работы в облачном окружении в Kaspersky Security Center Cloud Console
    - Шаг 1. Проверка требуемых плагинов и инсталляционных пакетов
    - Шаг 2. Выбор способа активации приложения
    - Шаг 3. Выбор облачного окружения и аутентификация
    - Шаг 4. Опрос сегментов и настройка синхронизации с облачным окружением
    - Шаг 5. Настройка Kaspersky Security Network для Kaspersky SIEM Cloud
    - Шаг 6. Создание первоначальной конфигурации защиты
  - Опрос сегмента сети с помощью Kaspersky Security Center Cloud Console
    - Добавление подключений для опроса облачных сегментов через Kaspersky Security Center Cloud Console
    - Удаление соединения для опроса облачных сегментов
    - Настройка расписания опроса с помощью Kaspersky Security Center Cloud Console
    - Просмотр результатов опроса облачного сегмента с помощью Kaspersky Security Center Cloud Console
    - Просмотр свойств облачных устройств с помощью OSMP Console
  - Синхронизация с облачным сегментом: настройка правила перемещения
  - Удаленная установка приложений на виртуальные машины Azure
- Настройка компонентов Kaspersky SIEM Cloud
  - Настройка параметров Ядра Kaspersky SIEM Cloud
  - Сбор и обогащение событий
    - Подключение источников событий
      - Kaspersky
        - Kaspersky Security Center (Сервер администрирования)
        - Kaspersky Security Center (MS SQL)
        - Kaspersky Web Traffic Security
        - Kaspersky Linux Mail Server
        - Kaspersky Secure Mail Gateway
        - Kaspersky Industrial CyberSecurity for Networks
        - Kaspersky Anti Targeted Attack Platform
        - Kaspersky Endpoint Security for Windows
        - Kaspersky Endpoint Security for Linux
      - Microsoft
        - Агент Kaspersky SIEM Cloud (WEC)
        - Агент Kaspersky SIEM Cloud (WMI)
        - Коннектор Event Tracing for Windows
        - Microsoft 365

- Unix и Linux
  - Auditd
  - FreeIPA
  - FreeRADIUS
  - ProFTPD
  - Vsftpd
  - HAProxy
  - Apache Tomcat
- Сетевые и защитные устройства
  - ИВК Кольчуга-К
  - КриптоПро NGate
  - Ideco UTM
  - McAfee Web Gateway
  - Positive Technologies Network Attack Discovery
  - Snort
  - Suricata
  - zVirt
  - VipNet TIAS
  - Zeek IDS
  - Angie
  - Dallas Lock 8
  - Единый центр управления Dallas Lock
- Базы данных и системы аудита СУБД
  - PostgreSQL
  - MariaDB Audit Plugin
  - Apache Cassandra
- Облачные и виртуальные платформы
  - Nextcloud
  - Yandex Cloud
  - VMware vCenter
  - Veeam Backup & Replication
- Почтовые и коллаборационные системы
  - CommuniGate Pro
  - Postfix
  - Sendmail
  - VK WorkSpace Mail
- Прочие специализированные системы
  - Codemaster Mirada
  - АПКШ Континент
  - Ansible
  - Grafana
  - TeamPass
  - SaltStack

Мониторинг источников событий

- Состояние источников
- Алгоритм применения политик мониторинга

Хранение событий
- О кластере ClickHouse
- Изменение хранилища
- Добавление пространства в хранилище
- Просмотр разделов хранилища
- Просмотр активных запросов в ClickHouse
- Холодное хранение событий
- Удаление дисков холодного хранения
- Отключение, архивирование и подключение партиций
- Резервное копирование партиций по расписанию
- Резервное копирование партиций вручную
- Восстановление партиций из резервной копии
- Импорт партиций из стороннего экземпляра Kaspersky SIEM Cloud
- Настройка хранилища S3
- Настройка сроков хранения и приоритетного удаления событий

Прием и нормализация событий
- Алгоритм работы коллектора
- Поддерживаемые источники событий
- Создание коллектора
- Установка коллектора в локальной инфраструктуре
- Обогащение событий данными Kaspersky CyberTrace
- Обеспечение бесперебойной работы коллекторов
- Агрегирование событий
- Нормализация событий
  - Настройка дополнительной нормализации событий
  - Переиспользование нормализаторов
  - Использование расширенной схемы событий для нормализации
    - Просмотр таблицы полей расширенной схемы событий
    - Добавление, изменение и удаление полей расширенной схемы событий
    - Импорт и экспорт полей расширенной схемы событий
- Использование коннектора
  - Параметры коннекторов
    - Коннектор, тип internal
    - Коннектор, тип tcp
    - Коннектор, тип udp
    - Коннектор, тип netflow
    - Коннектор, тип sflow
    - Коннектор, тип nats-jetstream
    - Коннектор, тип kafka
    - Коннектор, тип http
    - Коннектор, тип sql
    - Коннектор, тип file
    - Коннектор, тип 1c-log
    - Коннектор, тип 1c-xml
    - Коннектор, тип diode
    - Коннектор, тип ftp
    - Коннектор, тип sftp

Коннектор, тип nfs
Коннектор, тип wmi
Коннектор, тип wec
Коннектор, тип etw
Коннектор, тип snmp
Коннектор, тип snmp-trap
Коннектор, тип kata/edr
Коннектор, тип vmware
Коннектор, тип elastic
Коннектор, тип office365
Коннектор, тип dfi
Коннектор, тип universalAPI
Коннектор, тип smb
Коннектор, тип http-streaming
Предустановленные коннекторы
Использование точки назначения
Точка назначения, тип internal
Точка назначения, тип nats-jetstream
Точка назначения, тип tcp
Точка назначения, тип udp
Точка назначения, тип http
Точка назначения, тип diode
Точка назначения, тип kafka
Точка назначения, тип file
Точка назначения, тип storage
Точка назначения, тип correlator
Точка назначения, тип eventRouter
Использование прокси-сервера
Использование словаря
Настройка детектирующей логики и правил корреляции
Алгоритм работы коррелятора
Создание коррелятора
Правила корреляции
Работа с правилами корреляции
Правило корреляции, тип standard
Правило корреляции, тип simple
Правило корреляции, тип operational
Использование фильтров в правилах корреляции
Ограничение количества срабатываний правила корреляции
Переменные в корреляторах
Локальные переменные в группирующих и уникальных полях
Локальные переменные в селекторе
Локальные переменные в обогащении событий
Локальные переменные в обогащении активных листов
Свойства переменных
Требования к переменным

Функции переменных
Объявление переменных
Добавление временного списка исключений для корреляционного правила
Предустановленные правила корреляции
Пакеты правил корреляции
Корреляция с использованием активов и категорий активов
Техники и тактики MITRE ATT&CK
Импорт списка техник MITRE ATT&CK
Добавление в коррелятор правил обогащения MITRE
Привязка техник MITRE ATT&CK к правилам корреляции
Экспорт правил корреляции в MITRE ATT&CK Navigator
Конвертер правил Sigma
Подготовка правила Sigma
Поддерживаемые примеры конвертации правил Sigma
Правила сегментации
Создание правила сегментации
Привязка правил сегментации к правилам корреляции
Активные листы
Просмотр таблицы активных листов коррелятора
Добавление активного листа
Просмотр параметров активного листа
Изменение параметров активного листа
Дублирование активного листа
Удаление активных листов
Просмотр записей в активном листе
Поиск записей в активном листе
Добавление записи в активный лист
Дублирование записей в активном листе
Изменение записи в активном листе
Удаление записей в активном листе
Импорт записей в активный лист
Экспорт записей из активного листа
Предустановленные активные листы
Контекстные таблицы
Просмотр списка контекстных таблиц
Добавление контекстной таблицы
Просмотр параметров контекстной таблицы
Изменение параметров контекстной таблицы
Дублирование параметров контекстной таблицы
Удаление контекстной таблицы
Просмотр и поиск записей контекстной таблицы
Добавление, изменение и удаление записей в контекстной таблице
Экспорт данных из контекстной таблицы
Импорт данных в контекстную таблицу
Обогащение событий
Просмотр правил обогащения
Создание правила обогащения

- Привязка правил обогащения
- Управление правилами обогащения
- Добавление правил обогащения в свойствах коллектора
- Обогащение событий активами
- Обогащение событий геоданными
  - Формат геоданных
  - Конвертация геоданных из MaxMind и IP2Location
  - Импорт и экспорт геоданных
  - Сопоставление геоданных по умолчанию
- Получение и использование учетных записей Active Directory и Microsoft Entra ID
- Обогащение событий DNS-именами
- Обогащение событий с помощью словаря

Маршрутизация событий

- Запуск мастера установки маршрутизатора событий
  - Шаг 1. Общие параметры маршрутизатора событий
  - Шаг 2. Маршрутизация
  - Шаг 3. Проверка параметров
- Пример использования: коллектор передает события на маршрутизатор в центре обработки данных
- Пример использования: каскадное подключение маршрутизаторов событий

Создание и использование агентов Kaspersky SIEM Cloud

- Создание набора ресурсов для агента
- Управление подключениями для агента
- Создание сервиса агента в веб-консоли
- Автоматически созданные агенты
- Установка агента в сетевой инфраструктуре OSMP
  - Установка агента Kaspersky SIEM Cloud на устройствах Linux
  - Установка агента Kaspersky SIEM Cloud на устройствах Windows
- Обновление агентов
- Передача в Kaspersky SIEM Cloud событий из изолированных сегментов сети
  - Конфигурационный файл diode-агента
  - Описание полей секретов
  - Установка Linux-агента в изолированном сегменте сети
  - Установка Windows-агента в изолированном сегменте сети
- Настройка агента для получения событий Netflow из изолированного сегмента сети
- Получение служебных данных о событиях из изолированного сегмента
- Получение чувствительных данных по защищенному соединению
- Передача в OSMP событий с машин Windows
- Импорт файла со списком серверов для агентов WMI

Хранение конфиденциальной информации (секреты)

Работа с базой знаний

Управление ресурсами и сервисами

- Общие инструкции по работе с ресурсами
  - Создание, дублирование, перемещение, редактирование и удаление ресурсов
  - Привязка ресурсов к сервисам
  - Обновление предустановленных ресурсов
  - Экспорт ресурсов

Импорт ресурсов
Поиск ресурсов
Просмотр сервисов Kaspersky SIEM
Общие инструкции по работе с сервисами
Установка дополнительных ресурсов и сервисов
Версионирование ресурсов и сервисов
Просмотр графа зависимостей
Управление тегами
Управление папками
Уведомления Kaspersky SIEM Cloud
Подключение к SMTP-серверу
Изменение профиля пользователя
Управление сертификатами
Скачивание сертификатов
Изменение самоподписанного сертификата веб-консоли
Перевыпуск внутренних CA-сертификатов
Перевыпуск сертификата для отдельного сервиса
Интеграция с другими решениями
Kaspersky Automated Security Awareness Platform
Создание токена в KASAP и получение ссылки для API-запросов
Настройка интеграции в KUMA
Просмотр данных о пользователях KASAP и изменение учебных групп
Мониторинг и отчеты
Сценарий: мониторинг и отчеты
О типах мониторинга и отчетах
Панель мониторинга и виджеты
Использование панели мониторинга
Виджеты администрирования и защиты
Добавление виджета на информационную панель
Удаление виджета с информационной панели
Перемещение виджета на информационной панели
Изменение размера или внешнего вида виджета
Изменение параметров виджета
Веб-виджеты обнаружения и реагирования
Основные принципы работы с виджетами
Особенности отображения данных в виджетах
Создание виджета
Изменение виджета
Удаление виджета
Параметры виджетов
Виджет События
Виджет Активные листы
Виджет Контекстные таблицы
Пользовательский виджет Активы
Виджет Изображение
Виджет Текст
Другие виджеты

Фильтрация данных на виджетах
Фильтрация данных на одном виджете
Фильтрация данных на нескольких виджетах
Переход в связанную панель мониторинга
Информационная панель Обнаружение и реагирование
Создание макета панели мониторинга
Выбор макета панели мониторинга
Выбор макета панели мониторинга по умолчанию
Изменение макета панели мониторинга
Удаление макета панели мониторинга
Включение и отключение режима ТВ
Преднастроенные макеты панели мониторинга
О режиме Просмотра только панели мониторинга
Настройка режима Просмотра только панели мониторинга
Просмотр и сохранение ревизии политики
Сравнение ревизий политики
Откат изменений объекта к предыдущей ревизии
Отслеживание состояния сервисов
Просмотр метрик Kaspersky SIEM Cloud
Условия срабатывания алертов по метрикам Kaspersky SIEM Cloud
Срабатывание правил в режиме Интеллектуального обучения
Просмотр списка обнаружений, выполненных с помощью правил Адаптивного контроля аномалий
Добавление исключений в правила Адаптивного контроля аномалий
Отчеты администрирования и защиты
Использование отчетов
Шаблон отчета
Создание шаблона отчета
Просмотр и изменение свойств шаблона отчета
Удаление шаблонов отчетов
Универсальность шаблона отчетов
Экспорт отчета в файл
Генерация и просмотр отчета
Создание задачи рассылки отчета
Отчеты обнаружения и реагирования
Шаблон отчета
Создание шаблона отчета
Настройка расписания отчетов
Изменение шаблона отчета
Копирование шаблона отчета
Удаление шаблона отчета
Экспорт и импорт шаблона отчета
Универсальность шаблона отчетов
Сформированные отчеты
Просмотр отчетов
Создание отчетов
Сохранение отчетов

Обновление отчетов
Удаление отчетов
События и выборки событий
О событиях в Kaspersky SIEM Cloud
События компонентов Kaspersky SIEM Cloud
Структура данных описания типа события
События Сервера администрирования
Критические события Сервера администрирования
События отказа функционирования Сервера администрирования
События предупреждения Сервера администрирования
Информационные события Сервера администрирования
События Агента администрирования
События предупреждения Агента администрирования
Информационные события Агента администрирования
События отказа функционирования Агента администрирования
Использование выборок событий
Создание выборки событий
Изменение выборки событий
Просмотр списка выборки событий
Экспорт выборки событий
Импорт выборки событий
Просмотр информации о событии
Экспорт событий в файл
Просмотр истории объекта из события
Хранение информации о событиях для задач и политик
Удаление событий
Удаление выборок событий
Настройка срока хранения события
Блокировка частых событий
О блокировке частых событий
Управление блокировкой частых событий
Отмена блокировки частых событий
Обработка и хранение событий на Сервере администрирования
Уведомления и статусы устройств
Об уведомлениях
Просмотр уведомлений, требующих внимания
Просмотр системных уведомлений
Просмотр объявлений
Просмотр экранных уведомлений
О статусах устройства
Настройка переключения статусов устройств
Настройка параметров доставки уведомлений
Проверка распространения уведомлений
Параметры и переменные среды для описания события
Объявления "Лаборатории Касперского"
Об объявлениях "Лаборатории Касперского"
Выключение объявлений "Лаборатории Касперского"

Получение предупреждения об истечении срока лицензии
Cloud Discovery
Включение функции Cloud Discovery с помощью виджета
Добавление виджета Cloud Discovery в панель мониторинга
Просмотр информации об использовании облачных сервисов
Уровень риска облачных сервисов
Блокировка доступа к нежелательным облачным сервисам
Активные угрозы
Дезинфекция необработанного файла
Скачивание необработанного файла
Удаление файлов из раздела Активные угрозы
Работа с ревизиями объектов
Просмотр и сохранение ревизии политики
Сравнение ревизий политики
Откат изменений объекта к предыдущей ревизии
Использование Kaspersky SIEM Cloud
Обнаружение угроз
Работа с алертами
Об алертах
Модель данных алерта
Просмотр таблицы алертов
Просмотр деталей алерта
Назначение алертов аналитикам
Изменение статуса алерта
Создание алертов вручную
Связь алертов с инцидентами
Удаление связи алертов с инцидентами
Связывание событий с алертами
Удаление связи событий с алертами
Работа с алертами на графе расследования
Рекомендации по обработке отдельных типов алертов
IoA алерты
Работа с инцидентами
Об инцидентах
Модель данных инцидента
Создание инцидентов
Создание дочерних инцидентов
Просмотр таблицы инцидентов
Назначение инцидентов аналитикам
Изменение статуса инцидента
Изменение приоритета инцидента
Объединение инцидентов
Экспорт инцидентов в файл
Управление Service Level Agreement (SLA)
Создание Service Level Agreement (SLA)
Удаление Service Level Agreement (SLA)

- Работа с типами инцидентов
  - Просмотр таблицы типов инцидентов
  - Создание типов инцидентов
  - Изменение типов инцидентов
- Управление типами рабочих процессов
  - Просмотр таблицы рабочих процессов инцидентов
  - Предустановленные рабочие процессы инцидентов
  - Создание рабочих процессов инцидентов
  - Изменение рабочих процессов и статусов инцидентов
- Управление трудозатратами инцидентов
  - Добавление трудозатрат инцидентов
  - Изменения трудозатрат инцидентов
  - Удаление трудозатрат инцидентов
  - Создание и экспорт отчетов об инцидентах
- Настройка периода хранения алертов и инцидентов
  - Просмотр информации об активе
- Пример расследования инцидента с помощью Kaspersky SIEM
  - Условия возникновения инцидента
  - Шаг 1. Предварительная подготовка
  - Шаг 2. Назначение алерта пользователю
  - Шаг 3. Проверка на соответствие между сработавшим правилом корреляции и данными событий алерта
  - Шаг 4. Анализ информации об алерте
  - Шаг 5. Проверка на ложное срабатывание
  - Шаг 6. Определение критичности алерта
  - Шаг 7. Создание инцидента
  - Шаг 8. Расследование
  - Шаг 9. Поиск связанных активов
  - Шаг 10. Поиск связанных событий
  - Шаг 11. Запись причин инцидента
  - Шаг 12. Реагирование на инцидент
  - Шаг 13. Восстановление работоспособности активов
  - Шаг 14. Закрытие инцидента
- Поиск угроз
  - Типовые сценарии поиска угроз
  - Работа с событиями
    - Гранулярный доступ к событиям
    - Просмотр таблицы событий
    - Поиск и фильтрация событий
    - Создание SQL-запросов вручную
    - Формирование SQL-запроса с помощью конструктора
    - Формирование SQL-запроса с помощью SQL-функций Kaspersky SIEM Cloud
      - Использование набора функций enrich в SQL-запросах
      - Использование набора функций lookup в SQL-запросах
    - Просмотр сведений о событии
    - Сохранение и выбор конфигурации фильтра событий
    - Фильтрация событий по периоду
    - Экспорт событий

Экспорт событий в хранилище S3
Просмотр событий аудита и настройка уведомлений
Ретроспективное сканирование
Получение статистики таблицы событий
AI-сервисы
Использование AI-ассистента KIRA
Настройка интеграции с KIRA с использованием LLM-провайдера
Выполнение анализа с помощью KIRA
Возможные ошибки задачи Проанализировать с помощью KIRA
Генерация регулярных выражений с помощью KIRA
Обнаружение атак DLL Hijacking
Управление активами
Добавление категории активов
Настройка таблицы активов
Поиск активов
Экспорт данных об активах
Просмотр информации об активе
Добавление активов
Добавление информации об активах
Импорт информации об активах из Kaspersky Security Center
Импорт информации об активах из MaxPatrol
Импорт данных об активах из MaxPatrol VM
Параметры конфигурационного файла kuma-ptvm-vulnerable-assets-config-template.yaml
Импорт информации об активах из KICS for Networks
Примеры сравнения полей активов при импорте
Назначение активу категории
Изменение параметров активов
Архивирование активов
Удаление активов
Удаление категории активов
Массовое удаление активов
Обновление приложений сторонних производителей и закрытие уязвимостей на активах Kaspersky Security Center
Перемещение активов в выбранную группу администрирования
Аудит активов
Настройка аудита активов
Хранение и поиск событий аудита активов
Включение и выключение аудита активов
Настраиваемые поля активов
Реагирование
Правила реагирования для пользовательского скрипта
Правила сбора и анализа данных
Работа с правилами сбора и анализа данных
Настройка планировщика для правила сбора и анализа данных
Анализ объемов сетевого трафика
Устранение неисправностей
Известные проблемы и ограничения
Способы получения технической поддержки

Техническая поддержка через Kaspersky CompanyAccount
Журналы Kaspersky SIEM Cloud
Приложения
Модель данных нормализованного события
Настройка модели данных нормализованного события из KATA EDR
Модель данных актива
Модель данных учетной записи
Порты, используемые Kaspersky SIEM Cloud
События аудита Kaspersky SIEM Cloud
Пользователь изменил параметры набора полей для определения источников
Добавлен файл ключа
Резервный лицензионный ключ добавлен
Резервный лицензионный ключ удален
Приложение активировано с помощью кода активации
Срок действия лицензии продлен
Недействительный код активации
Код активации заблокирован
Код активации или файл ключа удален
Превышено количество EPS
Окончание срока действия лицензии и начало льготного периода
Окончание льготного периода
Добавлен код активации или файл ключа с истекшим сроком годности
Изменен набор пространств для разграничения доступа к событиям
Изменены пороговые значения для мониторинга сервисов
Изменены значения параметров Ядра Kaspersky SIEM Cloud
Базы GeoIP импортированы
Сервис создан
Сервис удален
Сервис перезагружен
Сервис перезапущен
Сервис запущен
Сервис сопряжен
Статус сервиса изменен
Партиция удалена пользователем
Партиция удалена автоматически по истечении срока хранения
Удаление партиции по абсолютному сроку хранения
Удаление партиции по относительному сроку хранения
Перемещение партиции в холодное хранилище
Перемещение партиции в холодное хранилище завершилось с ошибкой
Активный лист успешно очищен или операция завершилась с ошибкой
Элемент активного листа успешно изменен или операция завершилась с ошибкой
Элемент активного листа успешно удален или операция завершилась с ошибкой
Активный лист успешно импортирован или операция завершилась с ошибкой
Активный лист экспортирован
Контекстная таблица экспортирована
Контекстная таблица успешно импортирована или операция завершилась с ошибкой
Элемент контекстной таблицы успешно изменен или операция завершилась с ошибкой

- Элемент контекстной таблицы успешно удален или операция завершилась с ошибкой
- Контекстная таблица успешно очищена или операция завершилась с ошибкой
- Ресурс добавлен
- Ресурс удален
- Ресурс обновлен
- Импорт ресурсов
- Параметры обновлены
- Словарь успешно обновлен на сервисе или операция завершилась ошибкой
- Запись добавлена в словарь
- Запись успешно удалена из словаря или операция завершилась с ошибкой
- Создание поля расширенной схемы события
- Редактирование поля расширенной схемы события
- Импорт поля расширенной схемы события
- Импорт нормализатора с полем расширенной схемы события
- Удаление поля расширенной схемы события
- Отправлен запрос в KIRA
- Реагирование через KICS/KATA
- Реагирование через Kaspersky Automated Security Awareness Platform
- Реагирование через KEDR
- Импорт техник и тактик MITRE ATT&CK
- Зарегистрирован алерт Metrics для сервиса или операция завершилась с ошибкой
- Реагирование в Active Directory
- Резервное копирование партиций, восстановление из резервной копии, импорт партиций из сторонней установки Kaspersky SIEM Cloud
- Запрос на естественном языке отправленный для преобразования в SQL-запрос с использованием KIRA
- Попытка чтения событий
- Поисковый запрос отменен
- Ресурсы KEDR обновлены
- Задача обновления ресурсов KEDR завершена
- Поля события KEDR обновлены
- Файл localizations.json обновлен
- Правило привязано к коллектору
- Правило отвязано от коллектора
- Правило привязано к коррелятору
- Правило отвязано от коррелятора
- Экспорт ресурсов из Kaspersky SIEM Cloud
- Получение служебных данных о событиях из изолированного сегмента
- Ребалансировка хранилища запущена
- Ребалансировка успешно завершена
- Запрос остановки ребалансировки хранилища
- Ребалансировка завершилась ошибкой

Правила корреляции

Фильтры

Формат времени

Сопоставление полей предустановленных нормализаторов

Юридическая информация
Лицензирование решения Kaspersky SIEM Cloud
Управление лицензионными ключами
Лицензирование приложения Kaspersky Security Center Cloud Console
Лицензирование приложения Kaspersky Security Center Cloud Console
Использование Kaspersky Marketplace для выбора бизнес-решений
Лицензии и минимальное количество устройств для каждой лицензии
События превышения лицензионного ограничения
Способы распространения кодов активации на управляемые устройства
Добавление лицензионного ключа Сервера администрирования
Добавление лицензионного ключа в хранилище Сервера администрирования
Распространение лицензионного ключа на клиентские устройства
Автоматическое распространение лицензионного ключа.
Просмотр информации об используемых лицензионных ключах
Просмотр информации о лицензионных ключах приложения
Удаление лицензионного ключа Сервера администрирования
Удаление лицензионного ключа из хранилища
Просмотр списка устройств, на которых приложение "Лаборатории Касперского" не активировано
Отзыв согласия с Лицензионным соглашением
Продление срока действия лицензии приложений "Лаборатории Касперского"
Использование Kaspersky SIEM Cloud после истечения срока действия лицензии
Определения лицензирования
О лицензии
О Лицензионном сертификате
О лицензионном ключе
О коде активации
О подписке
Информация о стороннем коде
Уведомления о товарных знаках
The MITRE Corporation Terms of Use

Kaspersky SIEM Cloud

Обзор решения

О решении

Аппаратные и программные требования

Архитектура

Начало работы

Создание учетной записи

Создание рабочей области

Вход в веб-интерфейс решения

Активация и первоначальная настройка

Руководство администратора

Изменение ранее развернутой конфигурации

Управление пользователями и настройка доступа по ролям

Аудит и мониторинг сервисов

Руководство пользователя

Сбор и обработка событий

Подключение источников событий

Управление активами

Интеграция с другими решениями

Хранение событий

Прием и нормализация событий

Настройка детектирующей логики и правил корреляции

Обогащение событий

Анализ данных и работа с инцидентами безопасности

Пример расследования инцидента

Мониторинг безопасности

Реагирование

Работа с событиями

Работа с алертами

Работа с инцидентами

Использование AI-сервисов

О решении

Kaspersky SIEM Cloud (далее также "решение") – это решение класса SIEM, предназначенное для централизованного сбора, хранения и анализа событий информационной безопасности. Решение помогает выявлять подозрительную активность и инциденты безопасности, обеспечивает возможность визуализации накопленных данных, построения автоматизированных отчетов, а также обеспечивает аналитическую поддержку процессов мониторинга и расследования в инфраструктуре организации.

Решение построено на микросервисной архитектуре. Функциональность Kaspersky SIEM Cloud реализована в виде отдельных сервисов, которые можно разворачивать и настраивать независимо друг от друга. Это позволяет изменять конфигурацию решения в зависимости от особенностей инфраструктуры организации и масштабировать обработку событий.

Kaspersky SIEM Cloud разворачиваются в облачном окружении и предоставляются вам в качестве службы. Вам не нужно устанавливать Kaspersky SIEM Cloud на свой сервер. Вы управляете Kaspersky SIEM Cloud с помощью OSMP Console, которая обеспечивает взаимодействие между вашим устройством и Kaspersky SIEM Cloud через браузер.

Доступные функциональные возможности:

Потоковая корреляция в реальном времени и корреляция по индексированным данным

Kaspersky SIEM Cloud осуществляет централизованный сбор и анализ событий информационной безопасности, корреляцию событий в реальном времени и своевременное оповещение об инцидентах, а также позволяет анализировать накопленные данные и выполнять их группировку, агрегацию, нормализацию и корреляцию с помощью правил сбора и анализа данных.

Интеграция с Kaspersky Investigation and Response Assistant (KIRA)

Kaspersky SIEM Cloud поддерживает интеграцию с Kaspersky Investigation and Response Assistant (KIRA) – LLM-инструментом для расследования и приоритизации алертов. KIRA выполняет деобфускацию вывода командной строки, формирует развернутый анализ с кратким резюме для оперативного принятия решений, снижает количество ошибок при обработке инцидентов, уменьшает требования к квалификации аналитиков первой линии и сокращает время, затрачиваемое администраторами на анализ событий.

Панели мониторинга

Панели мониторинга предназначены для отслеживания состояния безопасности сети и представляют собой гибко настраиваемый набор виджетов, отображающих различную аналитику данных безопасности.

Сбор информации об активах и реагирование на инциденты

В Kaspersky SIEM Cloud реализован автоматический сбор инвентаризационной информации (установленное ПО, уязвимости, оборудование, владелец актива), которая может использоваться для корреляции событий ИБ с учетом контекста, а также при расследовании инцидентов. Возможность управления агентами, установленными на конечных устройствах, помогает в процессе реагирования на выявленные инциденты.

Ретроспективное сканирование

Kaspersky SIEM Cloud позволяет анализировать не только события в реальном времени, но и применять новые правила корреляции к событиям, произошедшим ранее. Это может быть полезным для более точной настройки правил корреляции, а также для ретроспективного анализа собранных данных.

Решение не предназначено для распространения на территории США. Функциональность продукта, включая получение обновлений кодовой базы, может быть недоступна при использовании программы на территории США.

Архитектура решения

Схема архитектуры включает следующие компоненты:

- Решение Kaspersky SIEM Cloud, развернутое в облачной инфраструктуре. Этот компонент обеспечивает выполнение следующих задач:
  - Управление решением с помощью пользовательского веб-интерфейса.
  - Получение событий с помощью *коллекторов*. Коллекторы могут быть установлены как в облачной инфраструктуре, так и локально, в инфраструктуре организации. Коллектор принимает и приводит события из разных источников к единой схеме данных, позволяет выполнить агрегацию событий по определенному признаку или их обогащение дополнительной информацией. Коллектор передает события в хранилище, коррелятор и/или сторонние сервисы для выявления алертов.
  - Корреляция событий. *Корреляторы* анализируют поступающие события и выявляют алерты в соответствии с логикой, описанной в корреляционных правилах. Для расширения корреляционного контекста могут применяться активные листы, контекстные таблицы и локальные переменные.
  - Хранение событий.
  - Управление сервисами и учетными записями пользователей решения.
  - Визуальный мониторинг работы решения.
  - Расследование угроз безопасности на основе полученных событий.

- *Маршрутизаторы событий*, которые принимают события от коллекторов и с учетом настроенных фильтров направляют события в заданных точки назначения.

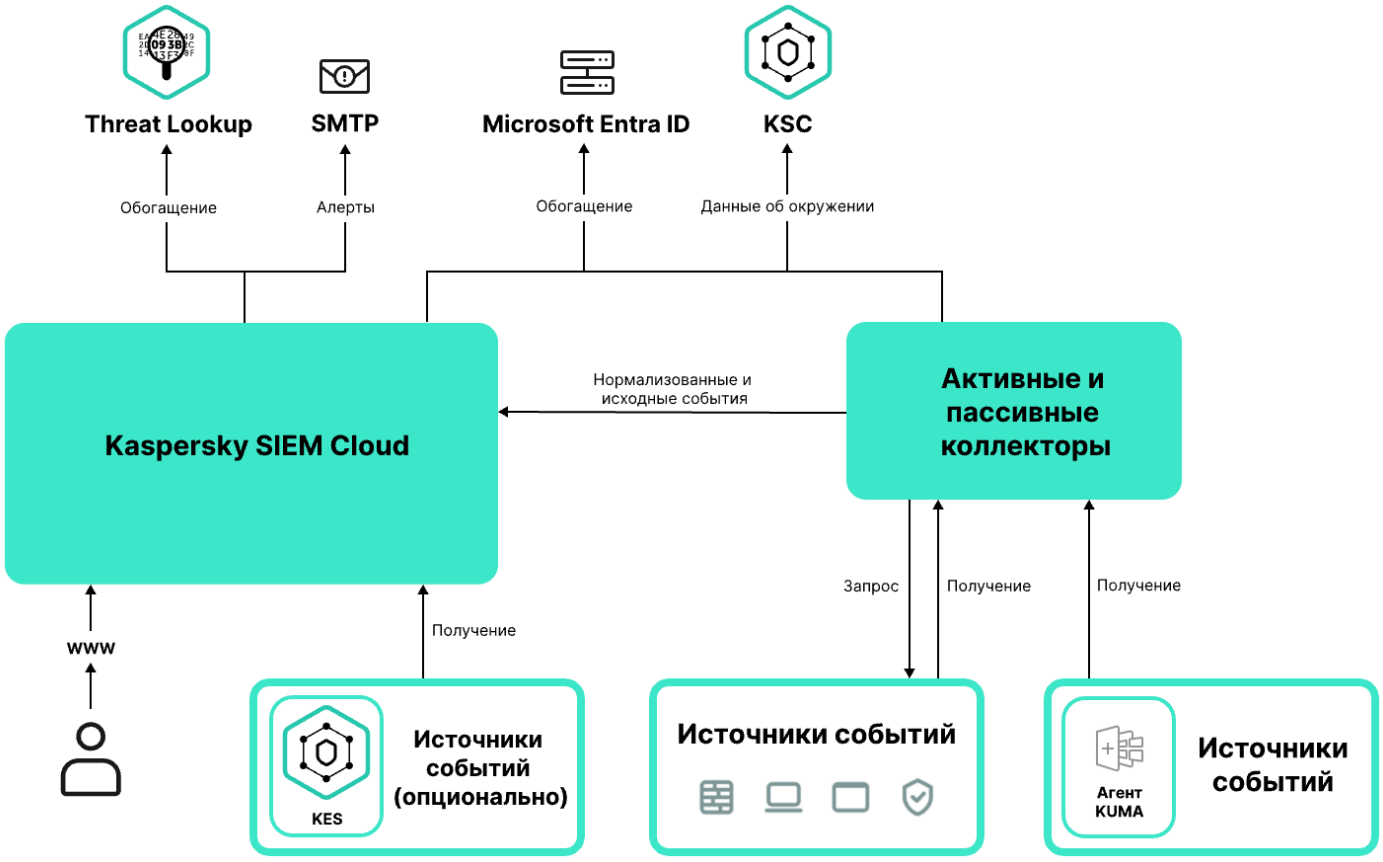
  Маршрутизатор событий не является обязательным сервисом. Он может потребоваться в компаниях с филиалами, когда между датацентром с корреляторами, хранилищами событий и отдаленным филиалом узкие или перегруженные каналы связи. В таком случае в датацентре можно установить маршрутизатор событий, а коллекторы отдаленного филиала настроить на отправку данных в маршрутизатор, а не по отдельности в корреляторы и хранилища. Это позволяет снизить нагрузку на сетевые каналы.

- *Агенты*, которые используются для пересылки сырых событий с серверов и рабочих станций под управлением операционных систем семейства Windows и Linux в точки назначения Kaspersky SIEM Cloud.

  При необходимости агент может использоваться для распределения потока событий между несколькими компонентами Kaspersky SIEM Cloud и автоматического переключения на резервный компонент в случае недоступности основного.

- Интеграции с другими решениями.

Все сервисы Kaspersky SIEM Cloud передают события между компонентами по надежным транспортным протоколам с возможностью использования шифрования. При недоступности точки назначения сервис сохраняет события в локальном буфере файловой системы и передает их после восстановления соединения. Размер буфера для временного хранения событий настраивается.



Архитектура Kaspersky SIEM Cloud

Аппаратные и программные требования

В этой статье указаны версии программного обеспечения, на которых приложение было протестировано и для которых гарантируется его корректная работа. Приложение также может работать с другими версиями программного обеспечения, но такие конфигурации не проходили полного цикла тестирования и не входят в список гарантированно поддерживаемых.

Консоль администрирования

Для работы с OSMP Console требуется только браузер.

> Вы можете использовать только одно окно или вкладку браузера для работы с OSMP Console.

Минимальное разрешение экрана составляет 1366x768 пикселей.

Требования к аппаратному и программному обеспечению устройства совпадают с требованиями к браузеру, который используется для работы с OSMP Console.

Браузеры:

- Google Chrome версии 154.0.8037.92 или выше
- Microsoft Edge версии 154.0.4258.62 или выше
- Safari 18.6 в macOS
- Mozilla Firefox Extended Support Release версии 140.17.0 или выше

Список операционных систем, поддерживаемых Агентом администрирования, см. в справке Kaspersky Security Center Cloud Console.

Аппаратные и программные требования для установки компонентов Kaspersky SIEM Cloud см. в статье Требования для локальных компонентов.

Аппаратные и программные требования к устройствам для установки агентов

Требования к устройствам для установки и работы агентов, которые передают данные в коллектор, приведены в следующих статьях:

- Требования к устройствам Windows для установки агентов.
- Требования к устройствам Linux для установки агентов.
- Требования к устройствам с операционными системами Oracle Linux, Astra Linux, Ubuntu, РЕД ОС, Мос ОС.

Требования к устройствам Windows для установки агентов

Для передачи данных в коллектор Kaspersky SIEM Cloud на устройствах сетевой инфраструктуры требуется установить агенты. Требования к устройствам Windows для установки и работы агентов Kaspersky SIEM Cloud приведены в этой статье.

Системные требования

Минимальные аппаратные требования:

- Процессор с частотой 1,4 ГГц или выше, 1 ядро.
- Оперативная память: 512 МБ.
- Объем свободного места на диске: 1 ГБ.

Поддерживаются следующие операционные системы:

- Microsoft® Windows® 2012 (поддерживается ограниченно).
- Microsoft Windows Server 2012 R2 (поддерживается ограниченно).
- Microsoft Windows Server 2016.
- Microsoft Windows Server 2019.
- Microsoft Windows Server 2022.
- Microsoft Windows Server 2025.
- Microsoft Windows 10.
- Microsoft Windows 11.

Требования к устройствам для установки агентов Kaspersky SIEM Cloud с коннекторами WEC, ETW и WMI

Агенты Kaspersky SIEM Cloud, установленные на устройствах с операционной системой Windows, могут использовать различные типы коннекторов для получения событий: WEC (Windows Event Collector), ETW (Event Tracing for Windows) и WMI (Windows Management Instrumentation). Производительность агентов и их влияние на систему зависят от ограничений Windows, а также от количества и типа обрабатываемых событий (см.таблицу ниже).

Требования к агентам по типам коннектора

Тип коннектора	Максимальная производительность (EPS)	Ограничения со стороны Windows	Ограничения со стороны Kaspersky SIEM Cloud	Рекомендуемая конфигурация агента	Загрузка процессора и ОЗУ
WEC	До 2500 событий в секунду	При записи в системные журналы (Application, System, Hardware Events) Windows ограничивает скорость записи примерно 2500 событиями в секунду. При одновременной записи в несколько журналов производительность снижается: до 1100 EPS при 2 журналах, до 800 EPS при 3 журналах, до 500 EPS при 4 журналах.	Агент может обрабатывать события в диапазоне 1500–2500 EPS без задержек.	Процессор: 1 ядро с 2 потоками или 2 vCPU. Оперативная память: 4 ГБ.	Средняя загрузка процессора агентом: до 0,18 (что эквивалентно примерно 0,28% от общей производительности системы). Использование ОЗУ – до 209 МБ.
ETW	До 700 событий в секунду	Поддерживается только один системный журнал: **Microsoft → Windows → DNS-Server**. Операционная система Windows не позволяет записывать более 700 событий в секунду в этот журнал.	Ограничений на стороне Kaspersky SIEM Cloud не выявлено, однако при EPS выше 700 агент не получает данные из-за ограничений Windows.	Процессор: 1 ядро с 2 потоками или 2 vCPU. Оперативная память: 4 ГБ.	Средняя загрузка процессора агентом: до 0,267 (что эквивалентно примерно 0,42% от общей производительности системы). Использование ОЗУ – до 186 МБ.
WMI	До 5000 событий в секунду	Обойти ограничения Windows можно за счет подключения нескольких устройств. Каждое дополнительное устройство увеличивает общий объем событий на 1000–1500 EPS.	При достижении отметки 5000 EPS агент начинает обрабатывать события с задержкой.	Процессор: 1 ядро с 2 потоками или 2 vCPU. Оперативная память: 4 ГБ.	Средняя загрузка процессора агентом: до 0,61 (что эквивалентно примерно 0,95% от общей производительности системы). Использование ОЗУ – до 311 МБ.

Требования к устройствам Linux для установки агентов

Для передачи данных в коллектор Kaspersky SIEM Cloud на устройствах сетевой инфраструктуры требуется установить агенты. Требования к устройствам Linux для установки и работы агентов Kaspersky SIEM Cloud приведены в этой статье.

Системные требования

Минимальные аппаратные требования:

- Процессор с частотой 1,4 ГГц или выше, 1 ядро.
- Оперативная память: 512 МБ.
- Объем свободного места на диске: 1 ГБ.

Поддерживаются следующие операционные системы:

- Oracle® Linux 8.x.
- Oracle Linux 9.x.

- Alma Linux 9.5.
- Astra Linux Special Edition РУСБ.10015-01 1.7.x (начиная с версии 2021-1126SE17 оперативное обновление 1.7.1) с установленной библиотекой glibc 2.28 (Debian GLIBC 2.28-10+deb10u4+ci202407161455+astra12).
- Astra Linux Special Edition РУСБ.10015-01 1.8.x (начиная с версии 2025-0114SE18MD срочное оперативное обновление 1.8.1.UU.2) с установленной библиотекой glibc 2.36 (Debian GLIBC 2.36-9+deb12u7+ci202405171200+astra5).
- CentOS Linux release 8.2.2004 (Core) с установленной библиотекой glibc 2.28 (GNU libc).
- CentOS Linux release 7.7.1908 (Core) с установленной библиотекой glibc 2.17 (GNU libc).
- Debian 12 с установленной библиотекой glibc 2.36 (Debian GLIBC 2.36-9+deb12u7).
- Red Hat Enterprise Linux 9.5 (Plow) с установленной библиотекой glibc 2.34 (GNU libc).
- Red OS 8.
- Rocky Linux 9.3 (Blue Onyx) с установленной библиотекой glibc 2.34 (GNU libc).
- Rocky Linux 9.5.
- SuSE 15.6.
- Ubuntu 24.04.2 LTS с установленной библиотекой glibc 2.39 (Ubuntu GLIBC 2.39-0ubuntu8.4).
- Ubuntu 22.04.4 LTS с установленной библиотекой glibc 2.35 (Ubuntu GLIBC 2.35-0ubuntu3.8).
- МосОС 15.5.

Требования к устройствам в зависимости от потока событий

Агенты Kaspersky SIEM Cloud, установленные на устройствах с операционной системой Linux, используют тип транспорта HTTP. Аппаратные требования для работы агентов Kaspersky SIEM Cloud зависят от потока событий (EPS) (см.таблицу ниже).

Аппаратные требования для работы агентов в зависимости от потока событий

	10 000 EPS	20 000 EPS	60 000 EPS	100 000 EPS
Процессор	3 ядра	5 ядер	6 ядер	6 ядер
Оперативная память	160 МБ	160 МБ	260 МБ	300 МБ

Требования к устройствам с операционными системами Oracle Linux, Astra Linux, Ubuntu, РЕД ОС, Мос ОС

В таблице ниже описаны требования при установке компонентов Kaspersky SIEM Cloud на устройствах с операционными системами Oracle Linux, Astra Linux, Ubuntu, РЕД ОС, Мос ОС.

	Oracle Linux	Astra Linux	Ubuntu	РЕД ОС	Moc ОС
Версия Python	С 3.6 по 3.12. Вы не можете одновременно использовать в одном экземпляре хосты с поддержкой Python до версии 3.6 включительно и Python версии 3.10 и выше.	С 3.6 по 3.12. Вы не можете одновременно использовать в одном экземпляре хосты с поддержкой Python до версии 3.6 включительно и Python версии 3.10 и выше.	С 3.6 по 3.12. Вы не можете одновременно использовать в одном экземпляре хосты с поддержкой Python до версии 3.6 включительно и Python версии 3.10 и выше.	С 3.6 по 3.12. Вы не можете одновременно использовать в одном экземпляре хосты с поддержкой Python до версии 3.6 включительно и Python версии 3.10 и выше.	С 3.6 по 3.12. Вы не можете одновременно использовать в одном экземпляре хосты с поддержкой Python до версии 3.6 включительно и Python версии 3.10 и выше.
Модуль SELinux	Выключен	Выключен	Выключен	Выключен	Выключен
Система управления пакетами	pip3	pip3	pip3	pip3	pip3

Основные пакеты	• tar
	• systemctl
	• netaddr
	• firewalld
	Подробнее об обновлении с операционной системы Oracle Linux 8.x до Oracle Linux 9.x.
	Вы можете установить пакеты с помощью следующих команд:
	`pip3 install netaddr`
	`yum install firewalld`
		• tar
		• systemctl
		• python3-apt
		• curl
		• libcurl4
		Вы можете установить пакеты с помощью команды:
		`apt install python3-apt curl libcurl4`
			• tar
			• systemctl
			• python3-apt
			• curl
			• libcurl4
			Вы можете установить пакеты с помощью команды:
			`apt install python3-apt curl libcurl4`
				• tar
				• systemctl
				• netaddr
				• firewalld
				Вы можете установить пакеты с помощью следующих команд:
				`pip3 install netaddr`
				`dnf install firewalld`
					• tar
					• systemctl
					• python3-rpm
					Вы можете установить пакет с помощью следующих команд:
					`zypper refresh`
					`zypper install python3-rpm`

Зависимые пакеты	Нет значения	• netaddr • python3-cffi-backend Вы можете установить пакеты с помощью команды: `apt install python3-netaddr python3-cffi-backend` Если вы планируете обращаться к базам данных Oracle DB из Kaspersky SIEM Cloud, вам нужно установить пакет Astra Linux libaio1.	• netaddr • python3-cffi-backend Вы можете установить пакеты с помощью команды: `apt install python3-netaddr python3-cffi-backend`	Нет значения	Нет значения

	Oracle Linux	Astra Linux	Ubuntu	РЕД ОС	Moc ОС
Уровень прав пользователя, необходимый для установки решения	Нет значения	Высокий уровень целостности (63)	Нет значения	Нет значения.	Нет значения

Пакеты, которые нужно установить на всех целевых машинах при развертывании компонентов Kaspersky SIEM Cloud в кластере Kubernetes	• iscsi-initiator-utils
	• wireguard-tools
	Перед установкой пакетов на операционной системе Oracle Linux вам нужно добавить репозиторий EPEL в качестве источника с помощью одной из следующих команд:
	`Для Oracle Linux 8`
	`sudo yum install oracle-epel-release-el8`
	`Для Oracle Linux 9`
	`sudo yum install oracle-epel-release-el9`
	Вы можете установить пакеты с помощью команды:
	`sudo yum install iscsi-initiator-utils wireguard-tools`
		• open-iscsi
		• wireguard
		• wireguard-tools
		Вы можете установить пакеты с помощью команды:
		`sudo apt install open-iscsi wireguard wireguard-tools`
			• open-iscsi
			• wireguard
			• wireguard-tools
			Вы можете установить пакеты с помощью команды:
			`sudo apt install open-iscsi wireguard wireguard-tools`
				• iscsi-initiator-utils
				Вы можете установить пакет с помощью следующей команды:
				`sudo apt install iscsi-initiator-utils`
				После установки пакета необходимо выполнить следующие команды:
				`sudo systemctl enable iscsid`
				`sudo systemctl start iscsid`
					Нет значения

Требования для локальных компонентов

Аппаратные требования

В таблице ниже приведены требования к оборудованию для установки компонентов Kaspersky SIEM Cloud в инфраструктуре организации в зависимости от количества поступающих в секунду событий (англ. events per second, далее EPS).

Аппаратные требования для установки компонентов Kaspersky SIEM Cloud

	До 3000 EPS	До 10 000 EPS	До 20 000 EPS	До 50 000 EPS
Требования к коллектору	-	-	Одно устройство. Характеристики устройства: • от 16 потоков или vCPU; • от 24 ГБ оперативной памяти; • от 500 ГБ в каталоге /opt; • тип хранилища данных – SSD; • скорость передачи данных – от 53 Мбит/с.	Два устройства. Характеристики каждого устройства: • от 16 потоков или vCPU; • от 24 ГБ оперативной памяти; • от 500 ГБ в каталоге /opt; • тип хранилища данных – SSD; • скорость передачи данных – от 134 Мбит/с.
Требования к маршрутизатору событий	-	Процессор: 3 ядра. Оперативная память: 240 МБ.	Процессор: 6 ядер. Оперативная память: 250 МБ.	Процессор: 9 ядер. Оперативная память: 7000 МБ.

Программные требования

Работа конвертера правил Sigma поддерживается на следующих операционных системах:

- Ubuntu 2024.
- Windows 10.
- Windows 11.
- РЕД ОС 7.
- РЕД ОС 8.
- Oracle Linux 8.3.
- Oracle Linux 9.3.

Совместимые приложения и решения

В этой статье указаны версии программного обеспечения, на которых приложение было протестировано и для которых гарантируется его корректная работа. Приложение также может работать с другими версиями программного обеспечения, но такие конфигурации не проходили полного цикла тестирования и не входят в список гарантированно поддерживаемых.

Kaspersky SIEM Cloud совместим со следующими приложениями и решениями:

- Kaspersky Endpoint Security для Linux 12.5.
- Kaspersky Endpoint Security для Windows 14.2.
- Kaspersky Endpoint Security для Mac 12.2.
- Kaspersky Automated Security Awareness Platform.
- Kaspersky Threat Intelligence Portal.
- Kaspersky Managed Detection and Response.

  Создание инцидента MDR из инцидента XDR на данный момент не поддерживается.

Настройка исключений в Kaspersky Endpoint Security для Linux

При установке компонентов Kaspersky SIEM Cloud и программы Kaspersky Endpoint Security для Linux на одном сервере возможны следующие проблемы:

- Каталог report.db может достигать больших размеров и занимать все дисковое пространство.
- Сканирование всех файлов Kaspersky SIEM Cloud, в том числе служебных, средствами Kaspersky Endpoint Security для Linux может снижать производительность системы.

Чтобы избежать этих проблем, выполните следующие действия:

1. Обновите программу Kaspersky Endpoint Security для Linux до версии 12.0 или выше.
2. Не включайте сетевые компоненты Kaspersky Endpoint Security для Linux.
3. Настройте следующие исключения в Kaspersky Endpoint Security для Linux:
   - Добавьте директорию `/opt/kaspersky/kuma` в общие исключения.
   - Добавьте директорию `/opt/kaspersky/kuma` в исключения для проверки по требованию.
   - Добавьте процесс `/opt/kaspersky/kuma/kuma` в исключения компонента Анализ поведения (Behavior Detection).

   Исключения нужно настроить на каждом сервере, на котором запускаются компоненты Kaspersky SIEM Cloud.

   > Исключение директории `/opt/kaspersky/kuma` распространяется на всю директорию Kaspersky SIEM Cloud и ее содержимое. Поэтому при добавлении новых компонентов или служебных директорий Kaspersky SIEM Cloud дополнительные исключения для отдельных директорий не требуются.

   Подробнее об исключениях из проверки см. онлайн-справку Kaspersky Endpoint Security для Linux.

Настройка исключений для экземпляра Kaspersky SIEM Cloud в конфигурации высокой доступности

Для экземпляра Kaspersky SIEM Cloud, развернутого в конфигурации высокой доступности, дополнительно настройте следующие исключения:

- Добавьте в исключения KESL TCP-трафик от и к порту 443 внутреннего Kubernetes API Service. По умолчанию в экземпляре Kaspersky SIEM Cloud с k0s используется адрес 10.96.0.1:443. Перехват или блокировка этого HTTPS-трафика средствами KESL может нарушить взаимодействие компонентов кластера с Kubernetes API и работу Calico CNI, что может привести к ошибкам запуска подов и нарушению работы кластера.

  IP-адрес 10.96.0.1 является значением `ClusterIP` по умолчанию и может отличаться в конкретной конфигурации кластера. Чтобы получить актуальный `ClusterIP`, на узле с ролью контроллера выполните команду:

  ```
  k0s kubectl get svc kubernetes -n default -o jsonpath='{.spec.clusterIP}{"\n"}'
  ```

  Используйте полученное значение `ClusterIP` для настройки исключения TCP-трафика на порту 443.

- Добавьте в общие исключения точку монтирования Kubernetes:

  ```
  /var/lib/k0s/kubelet/pods
  ```

О предоставлении данных

Kaspersky SIEM Cloud обрабатывает следующие данные.

Данные, необходимые для работы решения

Kaspersky SIEM Cloud – это комплексное программное решение, сочетающее в себе следующие основные функции:

- получение, обработка и хранение событий информационной безопасности;
- анализ и корреляция поступающих данных;
- поиск по полученным событиям;
- создание уведомлений о выявлении признаков угроз информационной безопасности;
- создание алертов и инцидентов для обработки угроз информационной безопасности;
- отображение информации о состоянии инфраструктуры заказчика на панели мониторинга и в отчетах;

- мониторинг источников событий;
- управление устройствами (активами): просмотр информации об активах, поиск, добавление, редактирование и удаление активов, экспорт данных об активах в файл формата CSV.

Для выполнения своих основных функций Kaspersky SIEM Cloud может принимать, хранить и обрабатывать следующую информацию:

- Данные об устройствах в сети организации.

  Сервер Ядра Kaspersky SIEM Cloud получает данные, если настроена соответствующая интеграция. Вы можете добавить активы в Kaspersky SIEM Cloud, импортировав активы из Kaspersky Security Center по расписанию.

  Kaspersky SIEM Cloud хранит следующие данные об устройствах:

  - Технические характеристики устройства.
  - Уязвимости, зафиксированные на активе.
  - Данные, специфичные для источника получения актива.
  - Категории устройства и уровень важности категории.

- Данные, содержащиеся в событиях от настроенных источников.

  В коллекторе настраивается источник событий, формируются события Kaspersky SIEM Cloud и передаются далее в другие сервисы Kaspersky SIEM Cloud. Иногда события могут поступать сначала в сервис агент, который передает события от источника в коллектор. Дополнительно можно настроить сохранение адреса или имя хоста сервера-агрегатора событий.

- Данные об источниках, с которых настроено получение событий.

  Это могут быть название источника, имя хоста, IP-адрес, политика мониторинга, назначенная этому источнику. В политике мониторинга указывается адрес электронной почты ответственного, кому будет отправлено уведомление при нарушении политики.

- Учетные записи пользователей: имя, логин, адрес электронной почты. Пользователь может просмотреть свои данные в профиле в Консоли Kaspersky SIEM Cloud.

- Параметры профиля пользователя:

  - Роли пользователя в Kaspersky SIEM Cloud. Пользователь может видеть назначенные ему роли.
  - Язык локализации, параметры уведомлений, отображение непечатаемых символов.

  Пользователь вводит эти данные в Консоли Kaspersky SIEM Cloud.

- Список категорий активов в разделе Активы, панель мониторинга по умолчанию, признак режима для панели мониторинга, SQL-запрос по событиям по умолчанию, пресет по умолчанию. Пользователь указывает эти параметры в соответствующих разделах Консоли Kaspersky SIEM Cloud.

- Информация о модели статусов инцидентов, включая предустановленную.

- Информация о типах инцидентов: общая информация о типе, включая имя и описания типа; связь типа и модели статусов инцидентов.

- Информация об учетных записях пользователей: полное имя и адрес электронной почты. Данная информация вводится пользователем в Консоли OSMP.

- Данные о личном токене доступа пользователя.
- Информация о сертификатах: сертификат сервера SIEM-коллектора.
- Данные об алертах и инцидентах:
  - Данные об алертах: сработавшие правила, соответствие матрице MITRE, статус алерта, резолюция, назначенный оператор или группа операторов, затронутые активы (устройства и учетные записи), наблюдаемые объекты (IP, MD5, SHA256, URL, DNS-домен или DNS-имя, имя пользователя, имя хоста), признак наличия устройств КИИ в алерте, комментарии и журнал изменений, файлы. Данная информация формируется в Консоли OSMP автоматически на основании корреляционных событий из Kaspersky Unified Monitoring and Analysis Platform. Данные об алертах хранятся в соответствии с заданным пользователем сроком хранения.
  - Данные об инцидентах: связанные алерты, дочерние инциденты, сработавшие правила, соответствие матрице MITRE, статус инцидента, резолюция, назначенный оператор или группа операторов, затронутые активы (устройства и аккаунты), наблюдаемый объект (из алерта), признак наличия устройств КИИ в инциденте, комментарии (включая комментарии на графе расследования), журнал изменений, файлы, тип инцидента, метрики по сортировке, реагированию, и разрешению инцидентов, причины просрочки метрик, Данная информация формируется в Консоли OSMP автоматически по правилам или вручную пользователем. Данные об инцидентах хранятся в соответствии с заданным пользователем сроком хранения.
- Данные о настройке правил формирования инцидентов из алертов: имя и условия срабатывания правила, шаблон имени нового инцидента, описание правила, приоритет запуска правила. Данная информация вводится пользователем в Консоли OSMP.
- Данные о шаблонах уведомлений: имя шаблона, тема сообщения, шаблон текста сообщения, описание шаблона и правила детектирования, при срабатывании которых будут отправляться уведомления, данные о выбранных технологиях детектирования, о которых нужно уведомлять пользователя и важности алертов и инцидентов. Данная информация вводится пользователем в Консоли OSMP.
- Данные о настройках интеграции (как с приложениями/службами "Лаборатории Касперского", так и со сторонними решениями, которые участвуют в сценариях Kaspersky XDR Expert):
  - Интеграция с Kaspersky Threat Intelligence Portal: API-токен доступа для подключения к Kaspersky Threat Intelligence Portal, срок хранения кэша, признак подключения через прокси, тип сервиса. Данная информация вводится пользователем в Консоли OSMP.
  - Интеграция с Kaspersky Automated Security Awareness Platform (KASAP): API токен доступа при подключении к KASAP, URL портала KASAP, Email Администратора KASAP, признак подключения через прокси. Данная информация вводится пользователем в Консоли OSMP.
  - Kaspersky Investigation & Response Assistant: сертификат и пароль или API токен для доступа к API LLM-провайдера. Данная информация вводится пользователем в Консоли OSMP.
- Файлы дампа, файлы трассировки и файлы журналов компонентов Kaspersky SIEM Cloud могут содержать персональные и конфиденциальные данные. Файлы дампа, файлы трассировки и файлы журналов хранятся в открытом виде на устройстве. Файлы дампа, файлы трассировки и файлы журналов не передаются в "Лабораторию Касперского" автоматически, но администратор может передать эти данные в "Лабораторию Касперского" вручную по запросу Службы технической поддержки для решения проблем в работе Kaspersky SIEM Cloud.
- События аудита. Kaspersky SIEM Cloud автоматически фиксирует события аудита.

- Журнал Kaspersky SIEM Cloud. Пользователь может включить ведение расширенных записей журналов в консоли Kaspersky SIEM Cloud. Записи журнала хранятся на устройстве пользователя, автоматическая передача данных отсутствует.
- Информация о принятии пользователем условий юридических соглашений с "Лабораторией Касперского".
- Данные по действующим лицензиям в Kaspersky SIEM Cloud.
- Любые данные, которые пользователь вводит в интерфейсе Kaspersky SIEM Cloud.

Перечисленные выше данные могут попасть в Kaspersky SIEM Cloud следующими способами:

- Пользователь вводит данные в консоли Kaspersky SIEM Cloud.
- Сервисы Kaspersky SIEM Cloud (агент или коллектор) получают данные при настроенном пользователем подключении к источникам событий.
- Через REST API Kaspersky SIEM Cloud.

  Перечисленные данные хранятся в базе данных Kaspersky SIEM Cloud (ClickHouse, SQLite). Пароли хранятся в зашифрованном виде (хранится хеш паролей).

"Лаборатория Касперского" обеспечивает защиту всех полученных данных в соответствии с законодательством и применимыми правилами "Лаборатории Касперского". Данные передаются по безопасным каналам связи.

Информацию о данных, необходимых для работы Kaspersky Managed Detection and Response, см. в справке решения.

Данные, передаваемые третьим сторонам

При использовании функциональности KIRA в Kaspersky SIEM Cloud с запросами пользователя в LLM-агент, с которым настроена интеграция, могут передаваться следующие данные.

Если вы используете функциональность расшифровки командной строки, полученной от источников событий, вместе с запросом будут отправляться из ПО в сторонний ИИ-сервис следующие данные:

- строка запроса;
- тип продукта;
- версия продукта;
- язык продукта;
- клиентский сертификат;
- идентификатор запроса;
- тип запроса.

Если вы используете функциональность генерации регулярных выражений с KIRA, вместе с запросом будут отправляться из ПО в сторонний ИИ-сервис следующие данные:

- список CEF-полей с их описанием
- примеры журналов, указанные пользователем;
- тип продукта;
- версия продукта;
- клиентский сертификат;
- идентификатор запроса.

Если вы используете функциональность автоматической генерации описаний алертов и инцидентов, вместе с запросом будут отправляться из ПО в сторонний ИИ-сервис следующие данные:

- имя алерта/инцидента;
- время поступления первого события;
- время поступления последнего события;
- приоритет (только для инцидентов);
- события, связанные с алертом или инцидентом;
- данные по алерту/инциденту:
- имя задачи;
- язык, на котором отправляется запрос и на котором ожидается получение ответа;
- источник;
- тип продукта;
- версия продукта;
- идентификатор запроса к сервису;
- тип запроса.

Если вы используете функциональность генерации поискового SQL-запроса на основе пользовательского запроса, сформированного на естественном языке, вместе с запросом будут отправляться из ПО в сторонний ИИ-сервис следующие данные:

- текст запроса пользователя;
- браузерное время пользователя;
- список edr полей с их описанием;
- список поддерживаемых функций ClickHouse;

- тип продукта;
- версия продукта;
- клиентский сертификат.

Начало работы

Следующие сценарии представляют собой пошаговые инструкции от приобретения Kaspersky SIEM Cloud до расследования инцидентов и поиска угроз.

Начните с установки и первоначальной настройки Kaspersky SIEM Cloud, изучите функции обнаружения и поиска угроз Kaspersky SIEM Cloud и ознакомьтесь с примером рабочего процесса расследования инцидентов.

Интерфейс Консоли OSMP

Управление Kaspersky SIEM Cloud осуществляется через интерфейс Консоли OSMP.

Окно Консоли OSMP содержит следующие элементы:

- главное меню в левой части окна;
- верхняя панель в верхней части окна;
- рабочая область в правой части окна.

Главное меню

Главное меню содержит следующие разделы:

- **Сервер администрирования**. Отображает имя Сервера администрирования, к которому вы сейчас подключены. Вы можете открыть свойства Сервера администрирования, нажав на имя Сервера администрирования.
- **Навигация консоли**. Отображает карту главного меню. Большинство отображаемых разделов можно добавить в закладки или установить в качестве домашней страницы. Раздел **Навигация консоли** установлен как домашняя страница по умолчанию. Вы можете изменить эти параметры.
- **Мониторинг**. Предоставляет обзор вашей инфраструктуры, статусов защиты и статистики, включая поиск угроз, алерты и инциденты и плейбуки. Также в этом разделе можно добавлять и настраивать ресурсы и службы Kaspersky SIEM Cloud.
- **Управление активами**. Инструменты для управления активами и оборудованием, а также политики приложений "Лаборатории Касперского".
- **Задачи**. Содержит инструменты для создания и запуска задач.
- **Пользователи и роли**. Позволяет управлять пользователями и ролями, настраивать права пользователей, назначать пользователям роли и связывать профили политик с ролями.
- **Хранилища**. Предоставляет вам доступ к хранилищам приложений.

- **Управление программным обеспечением**. Позволяет управлять приложениями "Лаборатории Касперского" и приложениями сторонних производителей, а также инсталляционными пакетами и патчами.

- **Операции**. Позволяет выполнять различные операции, включая лицензирование приложений, просмотр и управление зашифрованными дисками и событиями шифрования.

- **Обнаружение устройств и развертывание**. Позволяет опрашивать сеть для обнаружения клиентских устройств и распределять устройства по группам администрирования вручную или автоматически. В этом разделе также содержится информация о мастере развертывания защиты.

- **Marketplace**. Содержит информацию о бизнес-решениях "Лаборатории Касперского", позволяет выбрать нужные вам и перейти к приобретению этих решений на сайте "Лаборатории Касперского".

- **Параметры**. Содержит параметры интеграции Kaspersky SIEM Cloud с другими приложениями "Лаборатории Касперского" и позволяет вам создать API-токены. Он также содержит параметры, связанные с отображением элементов интерфейса в зависимости от используемых функций и с языком интерфейса. Кроме того, в этом разделе вы можете открыть окно настроек Kaspersky SIEM Cloud со всеми необходимыми параметрами, включая параметры конфигурации Kaspersky SIEM Cloud, настройки интеграции Kaspersky SIEM Cloud, управление лицензионными ключами и параметры доступа.

При необходимости вы можете свернуть главное меню до значков, нажав на значок стрелки (<<) внизу экрана.

Верхняя панель

Верхняя панель всегда отображается во всех разделах консоли и не может быть скрыта.

Левая часть панели содержит название и логотип приложения. Если вы нажмете на название или логотип приложения, откроется домашняя страница Консоли OSMP.

В центре панели находится раскрывающийся список с названием вашей текущей рабочей области. С помощью раскрывающегося списка можно выполнить одно из следующих действий:

- Переключиться на другую рабочую область, если она доступна.

- Вернуться к списку рабочих областей.

В правой части панели отображается значок уведомления (🔔), при нажатии на который открывается панель с уведомлениями.

Также в правой части панели отображается меню вашей учетной записи. Вы можете открыть меню, нажав на имя своей учетной записи, и выполнить одно из следующих действий, выбрав соответствующий пункт в раскрывающемся списке:

- Настроить параметры своей учетной записи.

  Если вы выберете пункт **Управление учетной записью**, вы будете перенаправлены на портал Kaspersky Account, где можно сменить пароль или адрес электронной почты, а также настроить двухэтапную аутентификацию.

- Выбрать язык интерфейса Kaspersky SIEM Cloud.

- Выбрать светлую тему интерфейса.

- Просмотреть информацию о Службе технической поддержки "Лаборатории Касперского".
- Перейти в справку Kaspersky SIEM Cloud.
- Просмотреть обучающие видеоролики о настройке и использовании Kaspersky SIEM Cloud и приложений безопасности.

  В браузере Mozilla Firefox, если вы воспроизводите видео в разделе **Обучающие материалы** во всплывающем окне, затем открываете видео в режиме картинка в картинке и закрываете видео во всплывающем окне, видео в режиме картинка в картинке также закрывается.

- Просмотреть информацию о доступных вам юридических документах для приложений "Лаборатории Касперского".
- Выйти из Kaspersky SIEM Cloud.

Рабочая область

В рабочей области отображается выбранная вами информация для просмотра в разделах окон интерфейса Консоли OSMP. Она также содержит элементы управления, которые можно использовать для настройки отображения информации.

Изменение домашней страницы OSMP Console

Домашняя страница отображается после входа в OSMP Console.

По умолчанию раздел **Навигация консоли** установлен как домашняя страница. Если необходимо, вы можете изменить домашнюю страницу.

Чтобы изменить домашнюю страницу:

1. В разделе **Навигация консоли** наведите курсор мыши на элемент, который вы хотите установить в качестве домашней страницы.
2. После того как отобразится значок дома (), нажмите на этот значок.

Домашняя страница изменена. На экране отобразится соответствующее сообщение. Элемент, выбранный в качестве домашней страницы, отмечен значком дома ().

Разделы **Marketplace** и **Параметры** невозможно установить в качестве домашней страницы.

Изменение языка интерфейса и темы

Вы можете выбрать язык и тему интерфейса Kaspersky SIEM Cloud.

Чтобы изменить язык интерфейса:

1. В верхней части панели нажмите на имя своей учетной записи.

   Отобразится меню вашей учетной записи.

2. В раскрывающемся списке выберите один из поддерживаемых языков.

Язык интерфейса изменен.

Чтобы изменить тему интерфейса:

1. В верхней части панели нажмите на имя своей учетной записи.

   Отобразится меню вашей учетной записи. По умолчанию выбрано – **Светлый режим**.

2. В раскрывающемся списке выберите одну из поддерживаемых тем.

Тема интерфейса изменена.

Добавление и удаление закладок

Вы можете добавить часто используемые разделы OSMP Console в закладки, чтобы быстро получать к ним доступ из раздела **Закладки** в главном меню.

> Если вы не добавили ни одного раздела в закладки, раздел **Закладки** не отображается в главном меню.

Вы можете добавить в закладки только те разделы, которые отображают страницы. Например, если вы перейдете в раздел **Управление активами** → **Управляемые устройства**, откроется страница с таблицей устройств, что означает, что вы можете добавить раздел **Управляемые устройства** в закладки. Если после выбора раздела в главном меню не отображается окно или элемент, то добавить такой раздел в закладки невозможно.

Чтобы добавить раздел в закладки:

1. В главном меню наведите курсор мыши на раздел, который вы хотите добавить в закладки.

2. После того как значок закладки (🔖) отобразится, нажмите на значок.

Раздел отображается в разделе **Закладки**.

Чтобы удалить раздел из закладок:

1. В главном окне приложения перейдите в раздел **Закладки**.

2. Наведите курсор мыши на раздел, который вы хотите удалить из закладок, и нажмите на значок закладки (🔖).

Раздел удален из закладок.

Вы также можете добавлять и удалять элементы из закладок в разделе **Навигация консоли**, наведя на них курсор мыши и нажав на значок закладки (). Выбранный элемент будет отмечен значком закладки () и отобразится в разделе **Закладки** главного меню. Если вы хотите удалить элемент из закладок, нажмите на значок закладки ().

Раздел **Закладки** отображается только в главном меню. Этот раздел никогда не отображается на странице **Навигация консоли**.

Возврат к списку рабочих областей

После открытия рабочей области вы можете вернуться на страницу портала, на которой отображаются созданные вами рабочие области. Если администраторы других рабочих областей предоставили вам доступ, назначив вашей учетной записи роль гостя или администратора, эти рабочие области также появятся на странице портала.

Чтобы вернуться к списку рабочих областей:

1. На верхней панели нажмите на раскрывающийся список с названием текущей рабочей области.
2. Выберите **Перейти на портал**.

   На странице портала отображается список рабочих областей.

Активация и первоначальная настройка Kaspersky SIEM Cloud

Прежде чем приступать к активации и первоначальной настройке Kaspersky SIEM Cloud, убедитесь, что вы выполнили следующие условия:

- Лицензионный ключ для Kaspersky SIEM Cloud добавлен в хранилище Сервера администрирования.
- Вашей учетной записи в Kaspersky Security Center Cloud Console назначена роль Главный администратор или у вашей учетной записи есть права в функциональной области **Общие функции: Интеграция приложений**.

Для начала работы с решением Kaspersky SIEM Cloud необходимо выполнить следующие шаги:

1 Активация Kaspersky SIEM Cloud

Чтобы активировать решение Kaspersky SIEM Cloud:

1. В консоли Kaspersky Security Center Cloud Console перейдите в раздел **Marketplace**.
2. В списке **Рекомендованные приложения** выберите Kaspersky SIEM Cloud.

   Откроется мастер активации Kaspersky SIEM Cloud.

3. На шаге **Общие** ознакомьтесь с описанием функциональности Kaspersky SIEM Cloud.

4. На шаге **Дополнение к решению** ознакомьтесь с текстом соглашения об использовании Kaspersky SIEM Cloud и примите его условия.

5. На шаге **Соглашение об обработке данных** ознакомьтесь с текстом соглашения о предоставлении данных и примите его условия.

6. На шаге мастера **Конфигурация SIEM** выберите способ развертывания конфигурации ресурсов SIEM:

   - Если вы хотите развернуть типовую конфигурацию ресурсов SIEM, выберите **Автоматическое развертывание**.

     В этом случае будут автоматически развернуты коллекторы, корреляторы и другие ресурсы SIEM, необходимые для приема и корреляции телеметрии от источников, предусмотренных правилами корреляции из SOC-пакета.

   - Если вы хотите настроить конфигурацию ресурсов SIEM самостоятельно, выберите **Развертывание вручную**.

     Подробнее об управлении ресурсами см. в разделе Общие инструкции по работе с ресурсами.

7. Нажмите на кнопку **Перейти к Расширенной облачной защите**.

   Откроется раздел **Расширенная облачная защита**. В этом разделе вы можете продолжить выполнение первоначальной настройки решения Kaspersky SIEM Cloud.

Решение Kaspersky SIEM Cloud активировано.

2 Первоначальная настройка

Первоначальная настройка решения выполняется в разделе **Параметры** → **Расширенная облачная защита**. После прохождения активации Kaspersky SIEM Cloud отображается в подразделе **Активные решения**.

Чтобы запустить первоначальную настройку Kaspersky SIEM Cloud, нажмите на кнопку **Открыть руководство по настройке**. Руководство по настройке позволяет последовательно выполнить все необходимые шаги.

После выполнения каждого шага руководства по настройке отмечайте его как выполненный с помощью флажка.

Чтобы выполнить первоначальную настройку решения Kaspersky SIEM Cloud, выполните следующие шаги в руководстве по настройке:

1. Обеспечьте сетевой доступ к коллекторам, которые принимают телеметрию от внешних источников.

   Для этого настройте параметры сетевого экрана и прокси-сервера, разрешив подключения к адресам коллекторов. Адреса коллекторов можно посмотреть в разделе **Ресурсы и сервисы**.

2. Настройте пользовательский доступ, назначив пользователям роли, необходимые для работы с Kaspersky SIEM Cloud.

   В зависимости от необходимых прав назначьте пользователю одну из следующих ролей: Администратор SOC, Младший аналитик, Аналитик 2-го уровня, Аналитик 1-го уровня, Менеджер SOC, Подтверждающий, Аудитор.

Первоначальная настройка Kaspersky SIEM Cloud завершена.

Типовая конфигурация решения

При выборе автоматического развертывания при активации решения Kaspersky SIEM Cloud развертывается в типовой конфигурации. При необходимости вы можете добавить в конфигурацию дополнительные ресурсы и сервисы. Дополнительные сервисы вы можете установить только при наличии у вас достаточного количества вычислительных единиц.

Типовая конфигурация решения включает в себя следующие ресурсы и сервисы Kaspersky SIEM Cloud:

- Коллекторы:
  - Коллектор [OOTB] Syslog-CEF с нормализатором. Для этого коллектора должен использоваться коннектор типа tcp, у параметра **Режим TLS** должно быть выбрано значение **Включено**.
  - Коллектор для событий Windows. Для этого коллектора должен использоваться коннектор типа tcp, у параметра **Режим TLS** должно быть выбрано значение **Включено**.
  - Коллектор для событий auditd. Для этого коллектора должен использоваться коннектор типа tcp, у параметра **Режим TLS** должно быть выбрано значение **Включено**, переключатель **Auditd** должен быть включен.
- Коррелятор [OOTB] OSMP Correlator. Коррелятор предназначен для обработки событий с коллекторов, установленных при типовой конфигурации решения. Параметры коррелятора доступны для изменения.
- Хранилище [OOTB] OSMP Storage.
- Правила корреляции:
  - Набор правил корреляции [OOTB] Multiple login attempts to OSMP console using the same account.
  - Набор правил корреляции [OOTB] OSMP Scanner detects.
- Точки назначения:
  - Точка назначения для хранилища [OOTB] OSMP Storage.
  - Точка назначения для коррелятора [OOTB] OSMP Correlator.

При переходе от решения Kaspersky SIEM Cloud к решению Kaspersky Next XDR Expert Cloud или Kaspersky EDR Expert Cloud типовая конфигурация будет автоматически дополнена недостающими сервисами и ресурсами в соответствии с типовой конфигурацией Kaspersky Next XDR Expert Cloud или типовой конфигурацией Kaspersky EDR Expert Cloud соответственно.

Проверка настройки Kaspersky SIEM Cloud

Чтобы убедиться, что Kaspersky SIEM Cloud правильно развернут и настроен, вы можете запустить на одном из активов тестовый исполняемый файл, который вызовет срабатывание IOA-правила. Если первоначальная настройка была выполнена правильно, срабатывание IOA-правила приведет к созданию алерта в списке алертов.

Прежде чем приступать к проверке, убедитесь, что выполнены следующие требования:

1. Пройден мастер активации Kaspersky SIEM Cloud.
2. Выполнена первоначальная настройка Kaspersky SIEM Cloud.

Чтобы проверить настройку Kaspersky SIEM Cloud:

1. На активе, на котором вы хотите выполнить проверку, создайте копию исполняемого файла и переименуйте ее:
   - На активе с операционной системой Windows скопируйте любой EXE-файл и переименуйте копию в `bss_ioa_test_name.exe`.
   - На активе с операционной системой Linux скопируйте любой бинарный файл (например, sleep) и переименуйте копию в `bss_ioa_test_name`.
2. Запустите переименованный файл.
3. В Kaspersky SIEM Cloud откройте список алертов в разделе **Мониторинг** → **Алерты**.

   В списке алертов отобразится IOA-алерт с указанным активом, на котором вы запустили файл. В деталях алерта будет указано IOA-правило `kl_demo_bss_test_name`. Если такой алерт создан, значит Kaspersky SIEM Cloud развернут и работает правильно.

Деактивация Kaspersky SIEM Cloud

Деактивировать Kaspersky SIEM Cloud может только пользователь с ролью Главного администратора.

Вы можете деактивировать решение Kaspersky SIEM Cloud, если больше не планируете его использовать. После деактивации решения будут удалены данные телеметрии, алерты, инциденты,а также пользовательские правила корреляции.

Чтобы деактивировать решение Kaspersky SIEM Cloud:

1. В консоли Kaspersky Security Center Cloud Console перейдите в раздел **Параметры** → **Расширенная облачная защита**.

2. В подразделе **Активные решения** найдите нужное решение и нажмите **Деактивировать**.

3. В открывшемся окне подтверждения введите код деактивации и нажмите **Деактивировать**.

Решение Kaspersky SIEM Cloud деактивировано.

Администрирование с помощью Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console — централизованная платформа управления и администрирования, которая лежит в основе облачного решения Kaspersky SIEM Cloud.

С помощью Kaspersky Security Center Cloud Console вы можете выполнять следующие действия:

- Устанавливать приложения "Лаборатории Касперского" на устройства вашей сети и управлять установленными приложениями.
- Формировать иерархию групп администрирования для управления набором клиентских устройств как единым целым.
- Создавать виртуальные Серверы администрирования и располагать их в иерархии.
- Защищать свои сетевые устройства, включая рабочие станции и серверы с помощью приложений "Лаборатории Касперского".
- Управлять доступом пользователей к функциональности Kaspersky SIEM Cloud.
- Удаленно управлять установленными приложениями "Лаборатории Касперского" на клиентских устройствах.
- Централизованно распространять лицензионные ключи приложений "Лаборатории Касперского" на клиентские устройства.
- Создавать и контролировать политики безопасности для устройств в вашей сети.
- Создавать и контролировать учетные записи пользователей.
- Создавать и управлять ролями пользователей (RBAC).
- Создавать и контролировать задачи приложений, установленных на устройствах сети.
- Просматривать отчеты о состоянии системы защиты для каждой организации индивидуально.

Руководство по усилению защиты

Kaspersky Security Center Cloud Console – это приложение, которое размещается и поддерживается "Лабораторией Касперского". Вам не нужно устанавливать Kaspersky Security Center Cloud Console на свой компьютер или сервер. Kaspersky Security Center Cloud Console позволяет администратору устанавливать приложения безопасности "Лаборатории Касперского" на устройства в корпоративной сети, удаленно запускать задачи проверки и обновления, а также управлять политиками безопасности управляемых приложений.

Приложение Kaspersky Security Center Cloud Console предназначена для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Приложение предоставляет администратору доступ к детальной информации об уровне безопасности сети организации. Kaspersky Security Center Cloud Console позволяет настраивать все компоненты защиты, построенной на основе приложений "Лаборатории Касперского".

Kaspersky Security Center Cloud Console имеет полный доступ к управлению защитой клиентских устройств и является важнейшим компонентом системы защиты организации. Поэтому для доступа к Kaspersky Security Center Cloud Console требуются усиленные меры защиты.

В Руководстве по усилению защиты описаны рекомендации и особенности настройки Kaspersky Security Center Cloud Console и его компонентов для снижения рисков его компрометации.

Руководство по усилению защиты содержит следующую информацию:

- настройка учетных записей для работы с Kaspersky Security Center Cloud Console;
- управление защитой клиентских устройств;
- настройка защиты управляемых приложений;
- передача информации в сторонние системы.

Перед началом работы с Kaspersky Security Center Cloud Console вам будет предложено ознакомиться с краткой версией Руководства по усилению защиты.

Обратите внимание, что вы не можете использовать Kaspersky Security Center Cloud Console, пока не подтвердите, что ознакомились с Руководством по усилению защиты.

Чтобы прочитать Руководство по усилению защиты:

1. Откройте Kaspersky Security Center Cloud Console и выполните вход. Kaspersky Security Center Cloud Console проверяет, подтвердили ли вы, что прочитали текущую версию Руководства по усилению защиты.

   Если вы еще не читали Руководство по усилению защиты, откроется окно с его краткой версией.

2. Выполните одно из следующих действий:

   - Если вы хотите просмотреть краткую версию Руководства по усилению защиты в виде текстового документа, перейдите по ссылке **Открыть в новом окне**.
   - Если вы хотите просмотреть полную версию Руководства по усилению защиты, перейдите по ссылке **Открыть Руководство по усилению защиты в онлайн-справке**.

3. После прочтения Руководства по усилению защиты установите флажок **Я подтверждаю, что полностью прочитал(а) и понимаю Руководство по усилению защиты** и нажмите на кнопку **Принять**.

Теперь можно работать с Kaspersky Security Center Cloud Console.

При появлении новой версии Руководства по усилению защиты Kaspersky Security Center Cloud Console предложит вам ее прочитать.

Планирование архитектуры Kaspersky Security Center Cloud Console

В общем случае на выбор архитектуры централизованного управления влияют расположение защищаемых устройств, доступы из смежных сетей, схемы обновления баз и другие параметры.

На начальном этапе проработки архитектуры мы рекомендуем ознакомиться с компонентами Kaspersky Security Center Cloud Console и их взаимодействием между собой, а также со схемами трафика данных и использования портов.

На основании этой информации нужно сформировать архитектуру, определяющую:

- организацию рабочих мест администраторов и способы подключения к Kaspersky Security Center Cloud Console;
- способ установки Агента администрирования и приложения защиты;
- использование точек распространения;
- использование виртуальных Серверов администрирования;
- использование иерархии Серверов администрирования;
- схему обновления антивирусных баз;
- другие информационные потоки.

Учетные записи и авторизация

Использование двухфакторной аутентификации Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console предоставляет пользователям возможность двухфакторной аутентификации.

Двухфакторная аутентификация позволяет повысить безопасность вашей учетной записи Kaspersky Security Center Cloud Console. Когда эта функция включена, каждый раз при входе в Kaspersky Security Center Cloud Console с помощью адреса электронной почты и пароля, вы вводите дополнительный одноразовый код безопасности. Вы можете получить одноразовый код безопасности по SMS или сгенерировать его в приложении для аутентификации (в зависимости от параметров двухфакторной аутентификации).

Категорически не рекомендуется устанавливать приложение для аутентификации на устройстве, с которого выполняется подключение к Kaspersky Security Center Cloud Console. Например, вы можете установить приложение для аутентификации на мобильном устройстве.

Запрет на сохранение пароля администратора

При работе с Kaspersky Security Center Cloud Console **категорически не рекомендуется** сохранять пароль администратора в браузере на устройстве пользователя.

Если браузер скомпрометирован, злоумышленник может получить доступ к сохраненным паролям. Также если устройство пользователя с сохраненными паролями украдено или потеряно, злоумышленник может получить доступ к защищенным данным.

Ограничить членство в роли "Главный администратор"

Рекомендуется ограничить членство пользователей в роли "Главный администратор".

При создании рабочей области пользователю по умолчанию присвоена роль Главный администратор. Это удобно для управления, но критично с точки зрения безопасности, так как роль "Главный администратор" имеет очень широкий набор привилегий. Назначение этой роли пользователям должно быть строго регламентировано.

Для организации администрирования Kaspersky Security Center Cloud Console рекомендуется обратить внимание на существующие роли для определенных должностей с заранее настроенным набором прав.

Настройка прав доступа к функциям приложения

Рекомендуется использовать возможности гибкой настройки прав доступа пользователей и групп пользователей к разным функциям Kaspersky Security Center Cloud Console.

Управление доступом на основе ролей позволяет создавать типовые роли пользователей с заранее настроенным набором прав и присваивать эти роли пользователям в зависимости от их служебных обязанностей.

Основные преимущества ролевой модели управления доступом:

- простота администрирования;
- иерархия ролей;
- принцип наименьшей привилегии;
- разделение обязанностей.

Вы можете воспользоваться встроенными ролями и присвоить их определенным сотрудникам на основе должностей либо создать полностью новые роли.

При настройке ролей требуется уделить особое внимание привилегиям, связанным с изменением состояния защиты Сервера администрирования и удаленной установкой стороннего программного обеспечения:

- Управление группами администрирования.
- Операции с Сервером администрирования.
- Удаленная установка.
- Изменение параметров хранения событий и отправки уведомлений.

  Эта привилегия позволяет настроить уведомления, которые запускают скрипт или исполняемый модуль на устройстве с Сервером администрирования при возникновении события.

Отдельная учетная запись для удаленной установки приложений

Помимо базового разграничения прав доступа, рекомендуется ограничить возможность удаленной установки приложений для всех учетных записей, кроме "Главного администратора" или иной специализированной учетной записи.

Рекомендуется использовать отдельную учетную запись для удаленной установки приложений. Вы можете назначить роль или разрешения отдельной учетной записи.

Управление защитой клиентских устройств

Правила автоматического перемещения устройств между группами администрирования

Рекомендуется ограничить использование правил автоматического перемещения устройств между группами администрирования.

Использование правил автоматического перемещения может привести к тому, что на устройство будут распространены политики, предоставляющие более широкий набор привилегий, чем было до перемещения.

Перемещение клиентского устройства в другую группу администрирования может привести к распространению на него параметров политик. Эти параметры политик могут быть нежелательны к распространению на гостевые и недоверенные устройства.

Эта рекомендация, не относится к первоначальному распределению устройств по группам администрирования.

Требования безопасности к устройствам с точками распространения и шлюзам соединений

Устройства с установленным Агентом администрирования могут использоваться в качестве точки распространения и выполнять следующие функции:

- Распространять обновления и инсталляционные пакеты, полученные от Сервера администрирования, на клиентские устройства в группе.
- Выполнять удаленную установку приложений сторонних производителей и приложений "Лаборатории Касперского" на клиентские устройства.
- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах.
- Выполняет роль прокси-сервера KSN для клиентских устройств.

С учетом доступных возможностей рекомендуется защитить устройства, выполняющие роль точек распространения, от несанкционированного доступа любого типа (включая физический доступ).

Настройка защиты управляемых приложений

Настройка защиты сети

Убедитесь, что вы успешно выполнили Сценарий первоначальной настройки Kaspersky Security Center Cloud Console. Этот сценарий также предусматривает выполнение шагов мастера первоначальной настройки.

При работе мастера первоначальной настройки создаются политики и задачи с параметрами по умолчанию. В вашей организации эти параметры могут оказаться не оптимальными или даже запрещенными. Поэтому рекомендуется настроить эти политики и задачи и создать дополнительные политики и задачи, если это необходимо для вашей корпоративной сети.

Установка пароля на выключение защиты и удаление приложения

Чтобы злоумышленники не могли отключить приложения безопасности "Лаборатории Касперского", рекомендуется установить пароль для выключения защиты и удаления приложений безопасности "Лаборатории Касперского". Вы можете установить пароль, например, для Kaspersky Endpoint Security for Windows, Агента администрирования и других приложений "Лаборатории Касперского". После включения защиты паролем рекомендуется заблокировать эти параметры, закрыв их "замком".

Указание пароля для запуска утилиты klmover и деинсталляции Агента администрирования

Настоятельно рекомендуется включить защиту паролем для запуска утилиты klmover и деинсталляции Агента администрирования. Чтобы включить защиту паролем, в параметрах политики Агента администрирования выберите параметр **Использовать пароль деинсталляции**.

При включении параметра **Использовать пароль деинсталляции** также включается защита паролем средствами Cleaner (cleaner.exe).

Утилита klmover используется только для перемещения управляемых устройств под управление виртуального Сервера администрирования. При установке на управляемое устройство Агента администрирования утилита klmover автоматически копируется в папку установки Агента администрирования.

Использование Kaspersky Security Network

Во всех политиках управляемых приложений и в свойствах Kaspersky Security Center Cloud Console рекомендуется использовать Kaspersky Security Network (KSN) и принять актуальное Положение о KSN. При обновлении Kaspersky Security Center Cloud Console вы также можете принять обновленное Положение о KSN.

Обнаружение новых устройств

Рекомендуется должным образом настроить параметры обнаружения устройств: настроить интеграцию с Active Directory и указать диапазоны IP-адресов для обнаружения новых устройств.

В целях безопасности вы можете использовать группу администрирования по умолчанию, в которую попадают все новые устройства, и применяемые к этой группе политики по умолчанию.

Передача событий в сторонние системы

Мониторинг и отчеты

Для своевременного реагирования на проблемы безопасности вы можете настроить функции мониторинга и параметры отчетов.

Экспорт событий в SIEM-системы

Для максимально быстрого выявления проблем безопасности до того, как будет нанесен существенный ущерб, рекомендуется использовать передачу событий в SIEM-систему.

Уведомление по электронной почте о событиях аудита

Для своевременного реагирования на возникновение нештатных ситуаций рекомендуется настроить отправку Kaspersky Security Center Cloud Console уведомлений о публикуемых им событиях аудита, критических событиях, событиях отказа функционирования и предупреждениях.

Поскольку события аудита являются внутрисистемными, они регистрируются редко и количество уведомлений о подобных событиях вполне приемлемо для почтовой рассылки.

Рекомендации по безопасности сторонних информационных систем

Рекомендации по безопасности CIS Benchmarks

При использовании версий операционных систем или платформ виртуализации, поддерживаемых Агентом администрирования, для тонкой настройки этих информационных систем рекомендуется применять методы защиты информации Center for Internet Security (CIS), если они существуют.

Center for Internet Security (CIS) – некоммерческая организация, занимающаяся повышением безопасности в области информационных технологий. В частности, CIS разрабатывает и распространяет стандарты безопасности, такие как CIS Controls и CIS Benchmarks. Эти стандарты представляют собой набор рекомендаций и практик по обеспечению безопасности информационных систем.

На портале CIS есть рекомендации для версий следующих информационных систем, поддерживаемых Агентом администрирования:

- Операционные системы следующих семейств:
  - Windows для рабочих станций
  - Windows для серверов
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- Платформы виртуализации VMware

Рекомендации по безопасности для операционной системы Astra Linux

При использовании операционной системы Astra Linux следует соблюдать рекомендации по безопасности, описанные в Red Book для соответствующей версии Astra Linux.

Рекомендации по использованию приложений безопасности "Лаборатории Касперского"

Использование пароля KLAdmin в Kaspersky Endpoint Security for Windows

Устройством с установленным приложением Kaspersky Endpoint Security for Windows могут пользоваться несколько пользователей с разным уровнем компьютерной грамотности. Если у пользователей есть неограниченный доступ к приложению Kaspersky Endpoint Security for Windows и его параметрам, общий уровень защиты устройства может быть снижен. Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security for Windows в соответствии с предоставленными им правами (например, разрешение на завершение работы приложения).

Один из способов ограничить доступ к приложению Kaspersky Endpoint Security for Windows и его параметрам – это использовать учетную запись KLAdmin. Учетная запись KLAdmin – это учетная запись администратора с неограниченным доступом к приложению Kaspersky Endpoint Security for Windows. Учетная запись KLAdmin имеет право выполнять любое действие, защищенное паролем, в Kaspersky Endpoint Security for Windows. Права для учетной записи KLAdmin не могут быть отозваны. Вы можете установить пароль для учетной записи KLAdmin в свойствах политики Kaspersky Endpoint Security for Windows. Администратор Kaspersky Endpoint Security for Windows несет полную ответственность за безопасное использование пароля для учетной записи KLAdmin. Если в вашей организации есть собственная политика использования паролей, следуйте указаниям этой политики.

Соблюдайте следующие рекомендации для защиты организации от кражи пароля KLAdmins:

- **Общие требования.**

  Не используйте имя учетной записи или часть имени в качестве пароля.

- **Требования к минимальной длине пароля.**

  Создайте пароль, который содержит не менее 10 символов.

- **Требования использования нескольких типов символов.**

  Задайте комплексный пароль, который содержит символы из разных категорий: буквы нижнего и верхнего регистров, цифры и специальные символы.

- **Требования к сроку действия пароля.**

  Установите минимальный срок действия пароля в 90 дней. Новый пароль не должен совпадать ни с одним из последних 24 паролей.

Обнаружение и реагирование на киберугрозы

Для эффективной защиты ИТ-инфраструктуры организации от сложных киберугроз, а также для автоматического обнаружения и анализа инцидентов безопасности рекомендуется использовать функции обнаружения и реагирования следующих решений "Лаборатории Касперского", которые можно интегрировать в интерфейс Kaspersky Security Center Cloud Console:

- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Managed Detection and Response
- Kaspersky Endpoint Detection and Response Expert

Сценарий: создание иерархии Серверов администрирования, управляемых с помощью Kaspersky Security Center Cloud Console

В этом сценарии описываются действия, которые необходимо выполнить для создания иерархии Серверов администрирования, управляемых с помощью Kaspersky Security Center Cloud Console, которая, таким образом, выполняет роль главного Сервера администрирования. Эта иерархия может впоследствии использоваться для переноса данных управляемых устройств и объектов из приложения Kaspersky SIEM Cloud в приложение Kaspersky Security Center Cloud Console, а также для управления подчиненными Серверами администрирования и устройствами с помощью Kaspersky Security Center Cloud Console.

Kaspersky Security Center Cloud Console может выполнять роль только главного Сервера администрирования, а локальные Серверы администрирования могут выполнять роль только подчиненных Серверов администрирования. Другие схемы иерархии недоступны.

Предварительные требования

Убедитесь, что выполнены следующие предварительные требования:

- Обновление Сервера администрирования, работающего локально, до версии 12 или выше.
- Установка Kaspersky Security Center Web Console на Сервера администрирования, работающего локально.
- Установка веб-плагинов для приложений, которыми вы планируете управлять с помощью Kaspersky Security Center Cloud Console.

- Обновление управляемых приложений до версий, поддерживаемых Kaspersky Security Center Cloud Console.

- Убедитесь, что в задаче Загрузка обновлений в хранилище Сервера администрирования на локальном Сервере администрирования главный Сервер администрирования не назначен в качестве источника обновлений. Измените параметры задачи, если это необходимо.

После того, как создана иерархия политики и задачи, которые действуют в Kaspersky Security Center Cloud Console, применяются на подчиненном Сервере администрирования, заменяя существующие политики и задачи. Чтобы избежать такой ситуации, удалите все политики и задачи Kaspersky Security Center Cloud Console перед созданием иерархии. Также вы можете изменить состояние каждой политики Kaspersky Security Center Cloud Console на **Неактивна** в ее параметрах и выключить параметр **Распространить на подчиненные и виртуальные Серверы администрирования** в свойствах каждой задачи Kaspersky Security Center Cloud Console.

Вы можете удалить иерархию Серверов администрирования в любое время, если это необходимо.

Этапы создания иерархии

Основной сценарий предусматривает подчиненный Сервер администрирования, к которому невозможно получить доступ из интернета. Однако набор действий некоторых из описанных ниже шагов может отличаться, если подчиненный Сервер администрирования доступен из интернета. Также в этом случае некоторые шаги нужно пропустить.

Создание иерархии Серверов администрирования состоит из следующих этапов:

1. **Получение сертификата подчиненного Сервера администрирования**

   Если подчиненный Сервер администрирования доступен из интернета, пропустите этот шаг.

   В приложении Kaspersky Security Center Web Console, работающем локально, откройте свойства Сервера администрирования и на вкладке **Общие** откройте раздел **Общие**. Перейдите по ссылке **Просмотреть сертификат Сервера администрирования**. Файл сертификата в формате CER автоматически сохраняется в папке, указанной в параметрах вашего браузера.

2. **Получение параметров подключения и сертификатов из Kaspersky Security Center Cloud Console**

   Если подчиненный Сервер администрирования доступен из интернета, пропустите этот шаг.

   В приложении Kaspersky Security Center Cloud Console откройте свойства Сервера администрирования на вкладке **Общие** и откройте раздел **Иерархия Серверов администрирования**. Отображаются следующие параметры подключения:

   - **HDS-адрес**

     Отображается веб-адрес, используемый для подключения к Hosted Discovery Service (HDS).

- **HDS-порт**

  Отображается номер порта, используемого для подключения к HDS.

Раздел также содержит две ссылки:

- **Просмотреть сертификат Сервера администрирования**

  При переходе по этой ссылке начинается загрузка открытого ключа экземпляра сертификата Kaspersky Security Center Cloud Console.

- **HDS-сертификат, выпущенный корневым центром сертификации**

  При переходе по этой ссылке начинается загрузка файла с расширением pem, который содержит список доверенных корневых сертификатов, подписанных аккредитованным Центром сертификации (CA). Этот файл предназначен для использования подчиненным Сервером администрирования: он требуется для проверки HDS-сертификата.

Скопируйте параметры подключения вручную, с помощью буфера обмена или любым другим удобным способом, и сохраните их в файл любого удобного формата. Перейдите по ссылке **Просмотреть сертификат Сервера администрирования** и дождитесь загрузки файла сертификата. Перейдите по ссылке **HDS-сертификат, выпущенный корневым центром сертификации** и дождитесь загрузки файла со списком доверенных корневых сертификатов, подписанных аккредитованным Центром сертификации. Оба файла сохраняются в папке, указанной в параметрах вашего браузера.

3. **Выбор подчиненного Сервера администрирования для подключения**

   В свойствах Сервера администрирования перейдите на вкладку **Серверы администрирования**. В иерархии групп администрирования установите флажок рядом с группой администрирования, в которой вы хотите разместить подчиненный Сервер администрирования со всеми его управляемыми устройствами. Нажмите на кнопку **Подключить подчиненный Сервер администрирования**.

   На открывшейся странице в поле **Имя подчиненного Сервера администрирования** укажите имя, под которым подчиненный Сервер администрирования должен отображаться в иерархии. Это имя используется только для вашего удобства и поэтому при необходимости может отличаться от реального имени подчиненного Сервера администрирования. Нажмите на кнопку **Далее**.

   Если подчиненный Сервер администрирования доступен из интернета, вы также должны указать адрес подчиненного Сервера администрирования в поле **Адрес подчиненного Сервера администрирования (необязательно)**.

   На следующей странице нажмите на кнопку **Обзор** и укажите файл с расширением pem, который вы сохранили с подчиненного Сервера администрирования. Нажмите на кнопку **Далее**.

4. **Включение и настройка параметров прокси-сервера**

   Действия этого этапа являются необязательными. Выполняйте их, только если в вашем случае соединение требует использование прокси-сервера.

   Нажмите на кнопку **Далее**. На странице **Параметры подключения и аутентификации**, вы можете включить и настроить использование прокси-сервера, если это необходимо. Установите флажок **Использовать прокси-сервер** и укажите следующие параметры прокси-сервера:

   - **Адрес прокси-сервера**

     Адрес прокси-сервера.

- **Имя пользователя**

  Имя пользователя для входа на прокси-сервер.

- **Пароль**

  Пароль для входа на прокси-сервер.

5. **Задание параметров аутентификации и добавление подчиненного Сервера администрирования в иерархию**

   Нажмите на кнопку **Далее**. На странице **Учетные данные подчиненного Сервера администрирования** укажите следующие параметры:

   - **Имя пользователя**

     Имя пользователя, под которым вы входите на подчиненный Сервер администрирования.

   - **Пароль**

     Пароль, используемый для входа на подчиненный Сервер администрирования.

   Нажмите на кнопку **Далее** и дождитесь появления подчиненного Сервера администрирования в иерархии.

   Если подчиненный Сервер администрирования доступен из интернета, он подключается к главному Серверу администрирования.

   > Если подчиненный Сервер администрирования доступен из интернета и соединение между двумя Серверами администрирования успешно установлено, пропустите все следующие шаги.

   Если к подчиненному Серверу администрирования невозможно получить доступ из интернета, он становится видимым, но для получения над ним контроля необходимо выполнить дополнительные действия на подчиненном Сервере администрирования.

6. **Настройка подключения в приложении Kaspersky Security Center Web Console, работающем локально**

   В приложении Kaspersky Security Center Web Console, работающей локально, откройте свойства Сервера администрирования и на вкладке **Общие** откройте раздел **Иерархия Серверов администрирования**. Установите флажок **Этот Сервер администрирования является подчиненным в иерархии**. В списке **Тип главного Сервера администрирования** выберите параметр **Kaspersky Security Center Cloud Console**.

   > Kaspersky Security Center Web Console проверяет, указан ли главный Сервер администрирования в качестве источника обновлений в задаче *Загрузить обновления в хранилище Сервера администрирования*. Если в качестве источника обновлений указан главный Сервер администрирования, вы получите соответствующее сообщение и ссылку на параметры задачи. Вы можете изменить параметры, а затем вернуться к созданию иерархии, или вы можете пропустить это действие и продолжить создание иерархии.

   В группе **Параметры для соединения между подчиненным и главным Серверами администрирования** укажите следующие параметры:

   - **Адрес HDS-сервера (для главного Сервера администрирования на Kaspersky Security Center Cloud Console)**

     Введите адрес HDS-сервера в формате полного доменного имени (FQDN); вы скопировали и сохранили этот адрес из свойств Сервера администрирования в Kaspersky Security Center Cloud Console.

- **Порты HDS-сервера**

  Введите номера портов HDS-сервера, которые вы скопировали и сохранили из свойств Сервера администрирования в Kaspersky Security Center Cloud Console.

7. **Добавление сертификатов на подчиненный Сервер администрирования**

   Нажмите на кнопку **Укажите сертификат главного Сервера администрирования** и укажите файл сертификата, который вы сохранили в свойствах Сервера администрирования в Kaspersky Security Center Cloud Console.

   Нажмите на кнопку **Укажите сертификат службы Hosted Discovery Service** и укажите файл .pem, который вы сохранили из свойств Сервера администрирования в Kaspersky Security Center Cloud Console.

   Если вы включили использование прокси-сервера при подключении подчиненного Сервера администрирования в Kaspersky Security Center Cloud Console, установите флажок **Использовать прокси-сервер** и укажите параметры прокси-сервера, как и в Kaspersky Security Center Cloud Console.

   Вы также можете установить флажок **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**, если подчиненный Сервер администрирования находится в демилитаризованной зоне (DMZ).

   Подчиненный Сервер администрирования подключается к главному Серверу администрирования.

Результаты

Выполнив вышеуказанные шаги, вы можете убедиться, что иерархия создана успешно:

- Активные политики главного Сервера администрирования вступают в силу на подчиненном Сервере администрирования. Задачи главного Сервера администрирования распространяются на подчиненный Сервер администрирования. Если параметр **Распространить на подчиненные и виртуальные Серверы администрирования** включен в параметрах групповой задачи, каждая такая задача также распространяется на подчиненный Сервер администрирования.

- Параметры политики, заблокированные для изменений на главном Сервере администрирования, отображаются как заблокированные для изменений во всех политиках на подчиненном Сервере администрирования.

- Политики, примененные на главном Сервере администрирования, отображаются в списке политик подчиненного Сервера администрирования (**Управление активами** → **Политики**).

- Групповые задачи, распространенные главным Сервером администрирования, отображаются в разделе **Задачи** в списке задач подчиненного Сервера администрирования.

- Политики и задачи, созданные на главном Сервере администрирования, невозможно изменить на подчиненном Сервере администрирования.

- В структуре групп администрирования Kaspersky Security Center Cloud Console подчиненный Сервер администрирования отображается в группе, выбранной вами при добавлении Сервера администрирования.

Перенос данных в Kaspersky Security Center Cloud Console

В этом разделе описывается перенос данных управляемых устройств из приложения Kaspersky Security Center версии 12 и выше, работающего локально, в Kaspersky Security Center Cloud Console.

Перенос данных из Kaspersky Security Center Linux в Kaspersky Security Center Cloud Console не поддерживается.

Способы переноса данных в Kaspersky Security Center Cloud Console

С помощью функции переноса данных вы можете перенести сетевые устройства из Kaspersky SIEM Cloud под управление Kaspersky Security Center Cloud Console. Управляемые устройства переключаются без потери основных параметров (например принадлежность к группам администрирования) и основных объектов (например, политик и задач, связанных с управляемыми приложениями).

Вы можете выбрать один из двух доступных способов переноса данных Серверов администрирования в Kaspersky Security Center Cloud Console:

- Перенос данных без иерархии Серверов администрирования:
  - Позволяет передавать управляемые устройства и связанные объекты в Kaspersky Security Center Cloud Console, даже если локальный Сервер администрирования не является подчиненным по отношению к Kaspersky Security Center Cloud Console.
  - Может потребоваться передача файлов (на съемном диске, по электронной почте, с помощью общих папок или любым другим удобным способом), если Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console запущены на разных физических устройствах.

  Вы также можете выполнить перенос данных с виртуальными Серверами администрирования, если они есть в вашей сети.

- Перенос данных с использованием иерархии Серверов администрирования:
  - Позволяет переносить управляемые устройства и связанные объекты в Kaspersky Security Center Cloud Console, используя только интерфейс Kaspersky Security Center Cloud Console, поэтому физическая передача файлов не требуется.
  - Требуется, чтобы Сервер администрирования, работающий локально, выполняющих роль подчиненного Kaspersky Security Center Cloud Console. Вы можете создать такую иерархию перед началом переноса данных.

Для полнодискового шифрования Kaspersky Security Center Cloud Console поддерживает только BitLocker.

Сценарий: перенос данных без иерархии Серверов администрирования

В этом разделе описывается перенос данных управляемых устройств и связанных с ними объектов (таких как политики, задачи, отчеты) из приложения Kaspersky Security Center Web Console, работающего локально, в Kaspersky Security Center Cloud Console. Вы можете включить одну группу администрирования в область переноса данных, чтобы восстановить эту группу администрирования в Kaspersky Security Center Cloud Console.

В эту группу должны входить управляемые устройства одной операционной системы. Если ваша сеть включает устройства с разными операционными системами или дистрибутивами Linux, распределите их по разным группам администрирования, а затем перенесите данные каждой группы отдельно.

После завершения переноса данных все Агенты администрирования, входящие в область переноса данных, обновляются и переходят под управление Kaspersky Security Center Cloud Console.

Шаги, перечисленные в этом разделе, описывают процесс переноса данных, выполняемый при отсутствии иерархии Серверов администрирования, то есть когда соединение между Kaspersky Security Center Cloud Console и приложением Kaspersky Security Center Web Console, работающем локально, не установлено.

Предварительные требования

Прежде чем начать, сделайте следующее:

- Обновите Сервер администрирования, работающий локально, до версии 14.2 или выше.
- Установите приложение Kaspersky Security Center Web Console версии 12.1 или выше.
- Обновите Агент администрирования на управляемых устройствах до версии 12 или выше.
- На устройствах с операционной системой Windows используйте Агент администрирования без пароля для деинсталляции.

  Если пароль уже задан, выполните одно из следующих действий в Kaspersky Security Center Web Console:

  - Выключите параметр **Использовать пароль деинсталляции** в свойствах политики Агента администрирования.
  - Удалите Агент администрирования удаленно с помощью задачи *Удаленная деинсталляция приложения*. В поле задачи **Приложение для деинсталляции** выберите значение **Агент администрирования Kaspersky Security Center**. Введите пароль для деинсталляции.
- Обновите управляемые приложения до версий, поддерживаемых Kaspersky Security Center Cloud Console.
- Убедитесь, что у вас есть политики для последних версий управляемых приложений. Если вы используете устаревшие политики, создайте политики для версий приложений, поддерживаемых Kaspersky Security Center Cloud Console.

- Чтобы использовать действующие политики, обновите веб-плагины для приложений, которыми вы планируете управлять с помощью Kaspersky Security Center Cloud Console.
- Удалите приложения "Лаборатории Касперского" с управляемых устройств, если эти приложения не поддерживаются Kaspersky Security Center Cloud Console.
- Расшифруйте все данные (на уровне диска или на уровне файлов), зашифрованные Kaspersky Endpoint Security для Windows на управляемых устройствах под управлением операционной системы Windows, и выключите функцию шифрования на управляемых устройствах с помощью политики приложения или локально. Дополнительную информацию см. в справке Kaspersky Endpoint Security для Windows.

  Если на устройстве с операционной системой Windows все еще хранятся какие-либо файлы или папки, зашифрованные с помощью Kaspersky Endpoint Security для Windows, обновление Агента администрирования будет отменено во время процесса переноса данных. Уведомление предложит вам расшифровать все данные на устройстве и отключить функцию шифрования.

Максимальное количество управляемых устройств на один Сервер администрирования в Kaspersky Security Center Cloud Console равно 25 000.

Этапы переноса данных

Перенос данных в Kaspersky Security Center Cloud Console включает в себя следующие этапы:

1. **Планирование области переноса данных и проверка предварительных требований**

   Оцените область переноса данных, то есть просмотрите группу администрирования для экспорта, и оцените количество управляемых устройств в ней. Также убедитесь, что все действия, перечисленные в качестве предварительных требований переноса данных, были успешно выполнены.

2. **Экспорт управляемых устройств, объектов и параметров из Kaspersky Security Center Web Console**

   Используйте мастер переноса данных приложения Kaspersky Security Center Web Console, работающего локально, для экспорта управляемых устройств вместе с их объектами.

   Максимальный размер файла экспорта составляет 4 ГБ.

3. **Импорт файла экспорта в Kaspersky Security Center Cloud Console**

   Перенесите информацию об управляемых устройствах и объектах в приложение Kaspersky Security Center Cloud Console. Для этого используйте мастер переноса данных Kaspersky Security Center Cloud Console, чтобы импортировать файл экспорта и создать автономный инсталляционный пакет Агента администрирования.

4. **Переустановка Агента администрирования на управляемых устройствах**

   Вернитесь в мастер переноса данных в экземпляре Kaspersky Security Center Web Console, работающего локально, чтобы создать задачу удаленной установки. Вы сможете использовать эту задачу (сразу или позже) для переустановки Агента администрирования на свои управляемые устройства и завершения процесса переноса данных.

Результаты

После завершения переноса данных вы можете убедиться, что перенос данных прошел успешно:

- Агент администрирования перестановлен на всех управляемых устройствах.
- Все устройства управляются через Kaspersky Security Center Cloud Console.
- Все параметры объектов, действовавшие до переноса данных, сохранились.

Мастер переноса данных

В этом разделе представлена информация о мастере переноса данных в Kaspersky Security Center Cloud Console и Kaspersky Security Center Web Console версии 12 и выше.

Шаг 1. Экспорт управляемых устройств, объектов и параметров из Kaspersky Security Center Web Console

Для переноса данных управляемых устройств из Kaspersky Security Center Web Console в Kaspersky Security Center Cloud Console необходимо сначала создать файл экспорта, содержащий информацию об иерархии групп администрирования на вашем текущем Сервере администрирования, работающем локально. Файл экспорта должен также содержать информацию об объектах и их параметрах. Файл экспорта будет использоваться для последующего импорта в Kaspersky Security Center Cloud Console.

Максимальный размер файла экспорта составляет 4 ГБ.

Чтобы экспортировать объекты и их параметры из Kaspersky Security Center Web Console:

1. В главном меню Kaspersky Security Center Web Console перейдите в раздел **Операции** → **Перенос данных**.
2. На странице приветствия мастера переноса данных нажмите на кнопку **Далее** Откроется страница **Управляемые устройства для экспорта**, на которой отображается вся иерархия групп администрирования соответствующего Сервера администрирования.
3. На странице **Управляемые устройства для экспорта** нажмите на значок шеврона (>) рядом с группой **Управляемые устройства**, чтобы раскрыть иерархию групп администрирования. Выберите группу администрирования, которую вы хотите экспортировать.

   После переноса данных из приложения Kaspersky Security Center, работающего локально, в Kaspersky Security Center Cloud Console, выполненного для двух групп администрирования, задачи удаленной установки для этих групп отображаются с одинаковыми именами.

4. Выберите управляемые приложения, политики и задачи, которые необходимо перенести в Kaspersky Security Center Cloud Console вместе с объектами группы администрирования. Чтобы выбрать управляемые приложения, чьи объекты необходимо экспортировать, установите флажки рядом с их именами в списке.

   Несмотря на то, что Сервер администрирования Kaspersky Security Center есть в списке, установка соответствующего флажка не приводит к экспорту политик Сервера администрирования.

   Чтобы убедиться, что управляемые приложения поддерживаются Kaspersky Security Center Cloud Console, перейдите по соответствующей ссылке. Ссылка перенаправит вас в раздел справки, содержащий список приложений, управляемых Kaspersky Security Center Cloud Console.

   > Если вы выберете приложения, которые не поддерживаются приложением Kaspersky Security Center Cloud Console, политики и задачи этих приложений будут экспортированы, а затем импортированы, но вы не сможете управлять ими в Kaspersky Security Center Cloud Console из-за недоступности плагинов.

5. Просмотрите список групповых объектов, экспортируемых по умолчанию, и укажите объекты, не относящиеся к группе, которые нужно экспортировать вместе с выбранной группой администрирования, если это необходимо. Настройте область экспорта, включив или исключив различные объекты, такие как глобальные задачи, пользовательские выборки устройств, отчеты, пользовательские роли, внутренние пользователи и группы безопасности, а также пользовательские категории программ. Эта страница содержит следующие разделы:

   - **Глобальные задачи**

     Список глобальных задач управляемых приложений, а также глобальных задач Агента администрирования.

     > Если выбранная вами глобальная задача применяется к определенной выборке объектов, эта выборка также будет экспортирована.

     > Несмотря на то, что глобальные задачи Сервера администрирования есть в списке, вы не можете их экспортировать; выбор этих задач не влияет на область экспорта. Задачи удаленной установки также не входят в область экспорта, так как соответствующие инсталляционные пакеты невозможно экспортировать.

   - **Выборки устройств**

     Список пользовательских выборок устройств.

   - **Reports**

     Редактируемый список отчетов для экспорта.

     > Если выбранный вами отчет применяется к определенной выборке объектов, эта выборка также будет экспортирована.

     > Kaspersky Security Center Cloud Console содержит такой же набор шаблонов отчетов, как и Kaspersky Security Center Web Console, поэтому вы можете выбрать для экспорта только те отчеты, которые вы создали вручную или перенастроили.

- **Групповые объекты**

  Список групповых объектов для экспорта по умолчанию. Следующие объекты, связанные с выбранной группой администрирования, будут экспортированы полностью по умолчанию:

  - Структура группы администрирования, то есть все вложенные группы выбранной группы администрирования.
  - Устройства, которые были включены в группы администрирования для экспорта.
  - Теги, назначенные экспортируемым устройствам.

    > Если тег был создан в Kaspersky Security Center Web Console, но никогда не был назначен никакому устройству, он не будет экспортирован. Также правила автоматического назначения тегов не будут экспортированы.

  - Групповые политики выбранных управляемых приложений.

    > Политики Сервера администрирования и политики Агента администрирования не экспортируются.

  - Групповые задачи выбранных управляемых приложений и групповые задачи Агента администрирования.

    > Задачи Сервера администрирования не экспортируются.

  Вы также можете запретить экспорт определенных типов объектов, не относящихся к группе:

  - Чтобы отменить экспорт пользовательских ролей (то есть созданных только пользователем), установите флажок **Исключить пользовательские роли из экспорта**.
  - Чтобы отменить экспорт для внутренних пользователей и групп безопасности, установите флажок **Исключить пользовательские роли и внутренние группы безопасности из экспорта**.
  - Чтобы отменить экспорт пользовательских категорий приложений, пополняемых вручную, установите флажок **Исключить пользовательские категории приложений из экспорта**.

Если вы переносите устройства с различными операционными системами в Kaspersky Security Center Cloud Console, объекты, не относящиеся к группе, необходимо перенести только один раз.

> Мастер переноса данных выполняет проверку общего количества управляемых устройств, включенных в выбранную группу администрирования. Если это количество превышает 10 000, появится сообщение об ошибке. Кнопка **Далее** остается неактивной до тех пор, пока количество управляемых устройств в выбранной группе администрирования будет меньше максимально допустимого значения.

6. После того как вы определили область переноса данных, нажмите на кнопку **Далее**, чтобы начать процесс экспорта. Откроется страница **Создание экспортного файла**, на которой можно просмотреть выполнение экспорта для каждого типа объектов, включенных в область переноса данных. Дождитесь, пока значки (🔄) рядом со всеми пунктами в списке объектов заменятся на зеленые флажки (✓). После того как экспорт заканчивается, файл экспорта автоматически загружается в папку загрузки, определенную в параметрах вашего браузера по умолчанию. Имя файла экспорта отображается в нижней части окна браузера.

7. После отображения страницы **Экспорт успешно завершен**, перейдите к следующему этапу, выполняемому в Kaspersky Security Center Cloud Console.

Если вы используете Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console на разных устройствах, необходимо скопировать файл экспорта на съемный диск или выбрать другие способы передачи файла.

Шаг 2. Импорт файла экспорта в Kaspersky Security Center Cloud Console

Чтобы передать информацию об управляемых устройствах, объектах и их параметрах, которые вы экспортировали из Kaspersky Security Center Web Console, вам нужно импортировать ее в приложение Kaspersky Security Center Cloud Console, развернутую в вашей рабочей области. Это позволит вам создать автономный инсталляционный пакет и использовать его для переустановки Агента администрирования на ваших управляемых устройствах.

Перед чем запустить мастер переноса данных в Kaspersky Security Center Cloud Console, убедитесь, что в процессе экспорта текущий язык локализации совпадает с языком локализации Kaspersky Security Center Web Console. При необходимости измените язык локализации.

Если вы ранее завершили мастер первоначальной настройки в рабочей области Kaspersky Security Center Cloud Console, то группа **Управляемые устройства** включает политики и задачи, созданные с параметрами по умолчанию. Удалите эти политики и задачи перед импортом тех, которые вы экспортировали из Kaspersky Security Center Web Console.

Чтобы импортировать файл экспорта в Kaspersky Security Center Cloud Console:

1. В главном меню Kaspersky Security Center Cloud Console, перейдите в раздел **Операции → Перенос данных**.

2. На странице приветствия мастера переноса данных нажмите на кнопку **Импортировать**. В открывшемся окне проводника выберите файл экспорта, перейдя в папку, в которой он был сохранен, и нажмите на кнопку **Открыть**. Дождитесь пока значок (🔄) рядом с файлом статуса загрузки изменится на зеленый флажок (✓).

3. Нажмите на кнопку **Далее**. Откроется следующая страница, на которой отображается вся иерархия групп администрирования Сервера администрирования в Kaspersky Security Center Cloud Console.

4. Установите флажок рядом с целевой группой администрирования, в которую должны быть восстановлены объекты группы, и нажмите на кнопку **Далее**. Мастер переноса данных отображает список инсталляционных пакетов Агента администрирования, доступных в Kaspersky Security Center Cloud Console.

5. Выберите инсталляционный пакет, содержащий соответствующую версию и локализацию Агента администрирования, и нажмите на кнопку **Далее**.

   Выберите инсталляционный пакет Агента администрирования для Windows, только если вы предварительно завершили мастер первоначальной настройки в рабочей области Kaspersky Security Center Cloud Console и если вы выполнили перенос данных для устройств под управлением операционной системы Windows.

   Подождите, пока мастер переноса данных создаст автономный инсталляционный пакет. Максимальный размер файла автономного инсталляционного пакета для Агента администрирования составляет 200 МБ.

   Файл распаковывается и автоматически загружается в папку загрузки, определенную в параметрах вашего браузера по умолчанию. Объекты, не относящиеся к группе, и объекты группы восстанавливаются в целевой группе администрирования.

   Когда импорт завершится, экспортированная структура групп администрирования, включая сведения об устройствах, появится в целевой группе администрирования, которую вы выбрали. Если имя восстанавливаемого объекта совпадает с именем существующего объекта, к восстановленному будет добавлен дополнительный суффикс.

   Если вы импортировали всю группу **Управляемые устройства**, рекомендуется переименовать только что импортированную подгруппу, чтобы избежать путаницы:

   a. Перейти в раздел **Иерархия групп**.

   b. Нажмите на имя подгруппы в дереве групп.

   c. В открывшемся окне свойств в поле **Имя** введите другое имя (например, "Перенесенные устройства").

   Рекомендуется проверить, успешно ли импортированы объекты (политики, задачи и управляемые устройства), входящие в область экспорта, в Kaspersky Security Center Cloud Console. Для этого перейдите в раздел **Управление активами** и проверьте, появились ли импортированные объекты в списках **Политики** и **Задачи**, а также в подразделах **Управляемые устройства**.

   Свернуть мастер переноса данных и выполнять любые параллельные операции во время импорта невозможно. Дождитесь, пока значки (🔄) рядом со всеми пунктами в списке объектов заменятся на зеленые флажки (✓) и импорт завершится. После этого устройства начинают переключаться на Kaspersky Security Center Cloud Console.

6. Нажмите на кнопку **Готово**, чтобы завершить работу мастера переноса данных.

7. Если вы хотите найти и снова загрузить автономный инсталляционный пакет, перейдите в раздел **Управление программным обеспечением** → **Инсталляционные пакеты** и нажмите на кнопку **Просмотреть список автономных пакетов**. В открывшемся списке выберите созданный вами автономный инсталляционный пакет и нажмите на кнопку **Скачать**.

   Если вы используете Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console на разных устройствах, вам нужно скопировать автономный инсталляционный пакет на съемный диск или выбрать другие способы передачи файла.

Шаг 3. Переустановка Агента администрирования на управляемых устройствах с помощью Kaspersky Security Center Cloud Console

После создания автономного инсталляционного пакета Агента администрирования вы можете приступить к созданию задачи удаленной установки. Выполнение этой задачи позволяет вам переустановить Агент администрирования на всех управляемых устройствах, чтобы эти устройства переключались под управление с помощью Kaspersky Security Center Cloud Console.

Чтобы снизить риск потери данных, рекомендуется сначала выполнить действия для небольшой группы администрирования, насчитывающей до 20 управляемых устройств (не включающих физических серверов), расположенных в корпоративной сети. После завершения этих действий проверьте, успешно ли завершилась повторная установка, и перейдите к повторной установке в полном объеме.

Чтобы создать задачу удаленной установки и переустановить Агент администрирования:

1. Вернитесь в мастер переноса данных в экземпляре Kaspersky Security Center Web Console, работающего локально.

   Рекомендуется использовать мастер переноса данных для создания задачи удаленной установки для переустановки Агента администрирования, как описано ниже. Если необходимо использовать пользовательскую задачу удаленной установки, требуется предварительно вручную создать пользовательский инсталляционный пакет из автономного инсталляционного пакета Агента администрирования. Обратите внимание, что при создании пользовательского инсталляционного пакета вам нужно указать ключ "-s" в командной строке исполняемого файла. Иначе переустановка Агента администрирования из этого пользовательского инсталляционного пакета завершится с ошибкой.

   В зависимости от текущего состояния мастера переноса данных вы можете выполнить одно из следующих действий:

   - Если вы не закрыли мастер переноса данных после экспорта и сеанс еще не истек, нажмите на кнопку **Вернуться к шагу 3 мастера переноса данных**. Установите флажок **Загрузить автономный инсталляционный пакет** и нажмите на кнопку **Выберите автономный инсталляционный пакет**. В открывшемся окне браузера укажите автономный инсталляционный пакет Агента администрирования.

   - Если по какой-либо причине вам необходимо снова запустить мастер переноса данных, установите флажок **Загрузить автономный инсталляционный пакет** и нажмите на кнопку **Выберите автономный инсталляционный пакет**. В открывшемся окне браузера укажите автономный инсталляционный пакет Агента администрирования. После этого мастер переноса данных снова отображает иерархию групп администрирования этого Сервера администрирования. Выберите ту же группу, для которой вы создали файл экспорта, и нажмите на кнопку **Далее**.

     Мастер переноса данных снова проверяет общее количество управляемых устройств, включенных в выбранную группу администрирования. Если это количество превышает 10 000, появится сообщение об ошибке. Кнопка **Далее** остается неактивной до тех пор, пока количество управляемых устройств в выбранной группе администрирования будет меньше максимально допустимого значения.

2. Дождитесь загрузки автономного инсталляционного пакета и нажмите на кнопку **Далее**. Мастер переноса данных создает пользовательский инсталляционный пакет и задачу удаленной установки для него. Область действия задачи будет включать группу администрирования, которую вы выбрали на странице **Управляемые устройства для экспорта**; по умолчанию для времени запуска задачи установлено значение запуска **Вручную**. Мастер переноса данных отображает процесс создания пакета. Дождитесь пока значки (↻) будут заменены зелеными флажками (✓) и нажмите на кнопку **Далее**.

3. При необходимости установите флажок **Запустить только что созданную задачу удаленной установки** (по умолчанию флажок снят) для устройств в выбранной группе администрирования Сервера администрирования, работающего локально, и всех его подгрупп. В этом случае устройства будут переключаться под управление Kaspersky Security Center Cloud Console, но только после завершения установки Агента администрирования. Полный путь будет отображен для группы администрирования, в которой будет выполняться задача.

   Задачу нужно запускать только после завершения импорта в Kaspersky Security Center Cloud Console. Иначе устройства могут дублироваться.

4. Нажмите на кнопку **Готово**, чтобы закрыть мастер переноса данных и запустить задачу удаленной установки для следующих целей:

   - Обновление экземпляров Агента администрирования.
   - Переключение экземпляров Агента администрирования под управление Kaspersky Security Center Cloud Console.

   Если вы оставили снятым флажок **Запустить только что созданную задачу удаленной установки**, вы можете запустить задачу позже, если это необходимо.

Вы можете проверить, что теперь вы можете управлять перенесенными экземплярами Агента администрирования с помощью Kaspersky Security Center Cloud Console. Для этого перейдите в раздел **Управление активами** → **Управляемые устройства**. Убедитесь, что на перенесенных управляемых устройствах есть значок подтверждения (⊘) в полях **Видимо в сети**, **Агент администрирования установлен** и столбцы **Агент администрирования запущен**. Также убедитесь, что на этих устройствах нет статуса с описанием *Давно не подключался*.

Перенос данных с иерархией Серверов администрирования

В этом разделе описывается перенос данных управляемых устройств и связанных с ними объектов из Kaspersky Security Center в Kaspersky Security Center Cloud Console. Процесс включает в себя иерархию: приложение Kaspersky Security Center Web Console, работающее локально, выполняет роль подчиненного Сервера администрирования, а Kaspersky Security Center Cloud Console выполняет роль главного Сервера администрирования.

Каждая группа администрирования, которую вы переносите в Kaspersky Security Center Cloud Console, должна содержать управляемые устройства одной операционной системы. Если ваша сеть включает устройства разных операционных систем, распределите их по разным группам администрирования, а затем перенесите каждую группу отдельно.

После завершения переноса данных все Агенты администрирования в группе, которая входит в область переноса данных, обновляются и переходят под управление Kaspersky Security Center Cloud Console.

Прежде чем начать, сделайте следующее:

- Обновите Сервер администрирования, работающий локально, до версии 14.2 или выше.
- Установите приложение Kaspersky Security Center Web Console версии 12.1 или выше.
- Обновите Агент администрирования на управляемых устройствах до версии 12 или выше.
- На устройствах с операционной системой Windows используйте Агент администрирования без пароля для деинсталляции.

  Если пароль уже задан, выполните одно из следующих действий в Kaspersky Security Center Web Console:

  - Выключите параметр **Использовать пароль деинсталляции** в свойствах политики Агента администрирования.
  - Удалите Агент администрирования удаленно с помощью задачи *Удаленная деинсталляция приложения*. В поле задачи **Приложение для деинсталляции** выберите значение **Агент администрирования Kaspersky Security Center**. Введите пароль для деинсталляции.
- Обновите управляемые приложения до версий, поддерживаемых Kaspersky Security Center Cloud Console.
- Убедитесь, что у вас есть политики для последних версий управляемых приложений. Если вы используете устаревшие политики, создайте политики для версий приложений, поддерживаемых Kaspersky Security Center Cloud Console.
- Чтобы использовать действующие политики, обновите веб-плагины для приложений, которыми вы планируете управлять с помощью Kaspersky Security Center Cloud Console.
- Удалите приложения "Лаборатории Касперского" с управляемых устройств, если эти приложения не поддерживаются Kaspersky Security Center Cloud Console.
- Расшифруйте все данные (на уровне диска или на уровне файлов), зашифрованные Kaspersky Endpoint Security для Windows на управляемых устройствах под управлением операционной системы Windows, и выключите функцию шифрования на управляемых устройствах с помощью политики приложения или локально. Дополнительную информацию см. в справке Kaspersky Endpoint Security для Windows.

  Если на устройстве с операционной системой Windows все еще хранятся какие-либо файлы или папки, зашифрованные с помощью Kaspersky Endpoint Security для Windows, обновление Агента администрирования будет отменено во время процесса переноса данных. Уведомление предложит вам расшифровать все данные на устройстве и отключить функцию шифрования.

Максимальное количество управляемых устройств на один Сервер администрирования в Kaspersky Security Center Cloud Console равно 25 000.

Чтобы выполнить перенос данных в Kaspersky Security Center Cloud Console:

1. Оцените область переноса данных, то есть просмотрите группу администрирования для экспорта, и оцените количество управляемых устройств в ней. Убедитесь, что все действия, перечисленные в качестве предварительных требований переноса данных, были успешно выполнены.
2. В Kaspersky Security Center Cloud Console перейдите на подчиненный Сервер администрирования для управляемых устройств, которые вы хотите перенести.

3. В главном окне приложения перейдите в раздел **Операции** → **Перенос данных**.

   Откроется страница приветствия мастера переноса данных.

4. На странице приветствия нажмите на кнопку **Далее**.

   Откроется страница **Управляемые устройства для экспорта**, на которой отображается вся иерархия групп администрирования подчиненного Сервера администрирования.

5. На странице **Управляемые устройства для экспорта** нажмите на значок шеврона (>) рядом с группой **Управляемые устройства** и раскройте иерархию групп администрирования. Выберите группу администрирования, которую вы хотите экспортировать.

   Мастер переноса данных выполняет проверку общего количества управляемых устройств, включенных в выбранную группу администрирования. Если это количество превышает 10 000, появится сообщение об ошибке. Кнопка **Далее** остается неактивной до тех пор, пока количество управляемых устройств в выбранной группе администрирования будет меньше максимально допустимого значения.

6. Выберите управляемые приложения, политики и задачи, которые необходимо перенести в Kaspersky Security Center Cloud Console вместе с объектами группы администрирования. Чтобы выбрать управляемые приложения, чьи объекты необходимо экспортировать, установите флажки рядом с их именами в списке.

   Несмотря на то, что Сервер администрирования Kaspersky Security Center есть в списке, установка соответствующего флажка не приводит к экспорту политик Сервера администрирования.

   Чтобы убедиться, что управляемые приложения поддерживаются Kaspersky Security Center Cloud Console, перейдите по ссылке. Ссылка перенаправит вас в раздел справки, содержащий список приложений, управляемых Kaspersky Security Center Cloud Console.

   Если вы выберете приложения, которые не поддерживаются приложением Kaspersky Security Center Cloud Console, политики и задачи этих приложений будут перенесены, но вы не сможете управлять ими в Kaspersky Security Center Cloud Console из-за недоступности плагинов.

7. Просмотрите список экспортируемых групповых объектов по умолчанию. При необходимости вы также можете указать объекты, не относящиеся к группе, которые будут экспортироваться вместе с выбранной группой администрирования, такие как глобальные задачи, пользовательские выборки устройств, отчеты, пользовательские роли, внутренние пользователи и группы безопасности, а также пользовательские категории программ, пополняемых вручную. Эта страница содержит следующие разделы:

   - **Глобальные задачи**

     Список глобальных задач управляемых приложений, а также глобальных задач Агента администрирования.

     Если выбранная вами глобальная задача применяется к определенной выборке объектов, эта выборка также будет экспортирована.

     Несмотря на то, что глобальные задачи Сервера администрирования есть в списке, вы не можете их экспортировать; выбор этих задач не влияет на область экспорта. Задачи удаленной установки также не входят в область экспорта, так как соответствующие инсталляционные пакеты невозможно экспортировать.

- **Выборки устройств**

  Список пользовательских выборок устройств.

- **Reports**

  Редактируемый список отчетов для экспорта.

  > Если выбранный вами отчет применяется к определенной выборке объектов, эта выборка также будет экспортирована.

  > Kaspersky Security Center Cloud Console содержит такой же набор шаблонов отчетов, как и Kaspersky Security Center Web Console, поэтому вы можете выбрать для экспорта только те отчеты, которые вы создали вручную или перенастроили.

- **Групповые объекты**

  Список групповых объектов для экспорта по умолчанию. Следующие объекты, связанные с выбранной группой администрирования, будут экспортированы полностью по умолчанию:

  - Структура группы администрирования, то есть все вложенные группы выбранной группы администрирования.
  - Устройства, которые были включены в группы администрирования для экспорта.
  - Теги, назначенные экспортируемым устройствам.

    > Если тег был создан в Kaspersky Security Center Web Console, но никогда не был назначен никакому устройству, он не будет экспортирован. Также правила автоматического назначения тегов не будут экспортированы.

  - Групповые политики выбранных управляемых приложений.

    > Политики Сервера администрирования и политики Агента администрирования не экспортируются.

  - Групповые задачи выбранных управляемых приложений и групповые задачи Агента администрирования.

    > Задачи Сервера администрирования не экспортируются.

Вы также можете запретить экспорт определенных типов объектов, не относящихся к группе:

- Чтобы отменить экспорт пользовательских ролей (то есть созданных только пользователем), установите флажок **Исключить пользовательские роли из экспорта**.
- Чтобы отменить экспорт для внутренних пользователей и групп безопасности, установите флажок **Исключить пользовательские роли и внутренние группы безопасности из экспорта**.
- Чтобы отменить экспорт пользовательских категорий приложений, пополняемых вручную, установите флажок **Исключить пользовательские категории приложений из экспорта**.

Если вы переносите устройства с различными операционными системами в Kaspersky Security Center Cloud Console, объекты, не относящиеся к группе, необходимо перенести только один раз.

8. После того как вы определили область переноса данных, нажмите на кнопку **Далее**, чтобы начать процесс экспорта. Откроется страница **Создание экспортного файла**, на которой можно просмотреть выполнение экспорта для каждого типа объектов, включенных в область переноса данных. Дождитесь пока каждый значок обновления (🔄) рядом с каждым пунктом в списке объектов заменится на зеленый флажок (✓). Экспорт заканчивается, файл экспорта автоматически сохраняется во временную папку. Откроется следующая страница, на которой отображается вся иерархия групп администрирования в приложении Kaspersky Security Center Cloud Console, выполняющее роль главного Сервера администрирования.

9. Установите флажок рядом с группой администрирования, в которую должны быть импортированы объекты группы, и нажмите на кнопку **Далее**. Файл распакован, а объекты, не относящиеся к группе, и объекты группы восстанавливаются в целевой группе администрирования.

   Если имя восстанавливаемого объекта совпадает с именем существующего объекта, к восстановленному будет добавлен дополнительный суффикс.

   Когда импорт завершится, экспортированная структура групп администрирования, включая сведения об устройствах, появится в целевой группе администрирования, которую вы выбрали. Объекты, не относящиеся к группе, также импортируются.

   Свернуть мастер переноса данных и выполнять любые параллельные операции во время импорта невозможно. Дождитесь, пока каждый значок обновления (🔄) рядом с каждым пунктом в списке объектов заменится на зеленый флажок (✓) и импорт завершится. После этого устройства начинают переключаться на Kaspersky Security Center Cloud Console.

10. После завершения импорта мастер переноса данных отобразит список инсталляционных пакетов Агента администрирования, доступных в Kaspersky Security Center Cloud Console для соответствующей операционной системы. Выберите инсталляционный пакет, содержащий соответствующую версию и локализацию Агента администрирования.

    Выберите инсталляционный пакет Агента администрирования для Windows, только если вы предварительно завершили мастер первоначальной настройки в рабочей области Kaspersky Security Center Cloud Console и если вы выполнили перенос данных для устройств под управлением операционной системы Windows.

11. Нажмите на кнопку **Далее**.

    Мастер переноса данных создает автономный инсталляционный пакет (или использует существующий) и пользовательский инсталляционный пакет на его основе, а также соответствующую задачу удаленной установки. Область действия задачи включает группу администрирования, выбранную вами на странице **Управляемые устройства для экспорта**. По умолчанию для времени запуска задачи установлено значение **Вручную**. Мастер переноса данных отображает процесс создания пакета.

12. Дождитесь, пока каждый значок обновления (🔄) заменится на зеленый флажок (✓) и нажмите на кнопку **Далее**.

13. При необходимости установите флажок **Запустить только что созданную задачу удаленной установки** (по умолчанию флажок снят) для устройств в выбранной группе администрирования приложения Kaspersky Security Center Web Console, работающего локально, и всех ее подгруппах. После завершения установки Агента администрирования вы можете управлять выбранными устройствами через Kaspersky Security Center Cloud Console. Полный путь отображается для группы администрирования, в которой будет выполняться задача.

    Задачу удаленной установки нужно запускать только после завершения импорта в Kaspersky Security Center Cloud Console. Иначе имена устройств могут дублироваться.

14. Нажмите на кнопку **Готово**, чтобы закрыть мастер переноса данных и запустить задачу удаленной установки для следующих целей:

    - Обновление экземпляров Агента администрирования.
    - Управление экземплярами Агента администрирования с помощью Kaspersky Security Center Cloud Console.

    Если вы оставили снятым флажок **Запустить задачу удаленной установки приложения**, вы можете запустить задачу позже, если это необходимо.

Вы можете проверить, что теперь вы можете управлять перенесенными экземплярами Агента администрирования с помощью Kaspersky Security Center Cloud Console. Для этого перейдите в раздел **Управление активами** → **Управляемые устройства**. Убедитесь, что на перенесенных управляемых устройствах есть значок подтверждения (⊘) в полях **Видимо в сети**, **Агент администрирования установлен** и столбцы **Агент администрирования запущен**. Также убедитесь, что на этих устройствах нет статуса с описанием *Давно не подключался*.

Сценарий: перенос данных устройств с операционными системами Linux или macOS

В этом разделе описан перенос данных управляемых устройств с операционными системами Linux или macOS из приложения Kaspersky Security Center Web Console, работающего локально, в Kaspersky Security Center Cloud Console. Основные сценарии переноса данных без иерархии Серверов администрирования и сценарий переноса данных с такой иерархией позволяют переносить все устройства и связанные с ними объекты в Kaspersky Security Center Cloud Console. Если в вашей сети есть устройства, работающие не только под операционной системой Windows, но и под Linux или macOS, вам необходимо переносить устройства каждого типа операционной системы отдельно. В результате вам придется выполнять перенос данных несколько раз.

Предварительные требования

Прежде чем начать, сделайте следующее:

- Обновите Сервер администрирования, работающий локально, до версии 12 патч A или выше.
- Установите приложение Kaspersky Security Center Web Console версии 12.1 или выше.
- Обновите Агент администрирования на управляемых устройствах до версии 12 или выше.
- Обновите управляемые приложения до версий, поддерживаемых Kaspersky Security Center Cloud Console.
- Убедитесь, что у вас есть политики для последних версий управляемых приложений. Если вы используете устаревшие политики, создайте политики для версий приложений, поддерживаемых Kaspersky Security Center Cloud Console.
- Чтобы использовать действующие политики, обновите веб-плагины для приложений, которыми вы планируете управлять с помощью Kaspersky Security Center Cloud Console.
- Удалите приложения "Лаборатории Касперского" с управляемых устройств, если эти приложения не поддерживаются Kaspersky Security Center Cloud Console, а затем замените удаленные приложения на поддерживаемые.

Максимальное количество управляемых устройств на один Сервер администрирования в Kaspersky Security Center Cloud Console равно 25 000.

Этапы переноса данных

Перенос данных в Kaspersky Security Center Cloud Console включает в себя следующие этапы:

1. **Группировка управляемых устройств по их операционным системам**

   Если в вашей сети есть устройства под управлением разных операционных систем (Windows, Linux и macOS), разместите устройства с каждой операционной системой в отдельной группе администрирования в Kaspersky Security Center Web Console. Также создайте группу администрирования для каждого дистрибутива Linux. Например, если у вас есть устройства Debian и Red Hat Linux, распределите их по разным группам администрирования. Это позволит вам успешно выполнить перенос данных, так как для разных операционных систем требуются разные инсталлированные пакеты Агента администрирования.

2. **Выполнение переноса каждой группы администрирования и ее объектов**

   Управляемые устройства каждой операционной системы должны переноситься отдельно, чтобы включать их политики и задачи. Например, если у вас есть устройства с Windows, macOS, Ubuntu и CentOS, сначала перенесите устройства с операционной системой Windows в Kaspersky Security Center Cloud Console, затем macOS, Ubuntu и, наконец, в CentOS. Вы можете переносить управляемые устройства в любом порядке.

Для этого выполните перенос данных без иерархии Серверов администрирования или перенос данных с такой иерархией, в зависимости от того, есть ли в вашей сети подчиненные Серверы администрирования. При переносе данных используйте инсталляционный пакет Агента администрирования, соответствующий операционной системе переносимых устройств. Например, выберите Агент администрирования Kaspersky Security Center 13.2 для устройств Linux, чтобы перенос данных прошел успешно.

Обратите внимание, что негрупповые объекты, такие как глобальные задачи, пользовательские выборки устройств или отчеты, необходимо перенести только один раз.

Результаты

После завершения переноса данных вы можете убедиться, что перенос данных прошел успешно:

- Требуемая версия Агента администрирования переустанавливается на каждом управляемом устройстве под управлением операционной системы Linux или macOS.
- Все устройства с операционными системами Linux или macOS управляются через Kaspersky Security Center Cloud Console.
- Все параметры объектов, действовавшие до переноса данных, сохранились.

Сценарий: обратный перенос данных из Kaspersky Security Center Cloud Console в Kaspersky Security Center

Вам может потребоваться перенести данные управляемых устройств из Kaspersky Security Center Cloud Console на Сервер администрирования Kaspersky Security Center. Этот процесс можно использовать для отмены переноса данных в Kaspersky Security Center Cloud Console.

Предварительные требования

Убедитесь, что выполнены следующие предварительные требования:

- Приложение Kaspersky Security Center Cloud Console доступно и к нему подключены управляемые устройства.
- Сервер администрирования Kaspersky Security Center 14.2 (или выше) доступен и имеет инсталляционный пакет Агента администрирования версии 13 или выше.

Этапы обратного переноса данных

Обратный перенос данных включает в себя следующие этапы:

1. **Создание автономного инсталляционного пакета Агента администрирования на Сервере администрирования Kaspersky Security Center, работающего локально**

На Сервере администрирования Kaspersky Security Center работающего локально, создайте автономный инсталляционный пакет Агента администрирования.

В процессе создания вы можете выбрать параметр **Перемещать нераспределенные устройства в эту группу** и указать группу администрирования, в которую вы хотите переместить Агенты администрирования после установки. Если вы указали группу администрирования, будет создано правило автоматического перемещения устройств, которое переместит в целевую группу администрирования все Агенты администрирования с этим автономным инсталляционным пакетом.

Чтобы обеспечить обратный перенос данных без ошибок, убедитесь, что вы выбрали версию Агента администрирования не ниже, чем версия, используемая в Kaspersky Security Center Cloud Console.

2. **Создание пользовательского инсталляционного пакета в Kaspersky Security Center Cloud Console**

   В Kaspersky Security Center Cloud Console создайте пользовательский инсталляционный пакет на основе автономного инсталляционного пакета, который вы создали и сохранили на Сервере администрирования Kaspersky Security Center, запущенного локально.

   Чтобы включить установку пакета в тихом режиме, в поле **Параметры запуска исполняемого файла** укажите ключ `-s`.

3. **Создание задачи удаленной установки**

   В Kaspersky Security Center Cloud Console создайте задачу удаленной установки с помощью созданного вами пользовательского инсталляционного пакета.

4. **Запуск задачи удаленной установки приложения**

   Запустите задачу удаленной установки, которую вы создали. Задача инициирует переустановку всех Агентов администрирования в указанной группе администрирования; задача также переключает Агенты администрирования под управление Сервера администрирования Kaspersky Security Center, работающего локально, путем изменения адреса подключения и других параметров подключения.

   Если вы не указали никакую целевую группу администрирования при создании автономного инсталляционного пакета, все устройства будут перемещены в группу **Нераспределенные устройства**.

Результаты

После завершения переноса данных вы можете убедиться, что перенос данных прошел успешно:

- Все устройства в области действия задачи удаленной установки, которые ранее управлялись через Kaspersky Security Center Cloud Console, теперь управляются Сервером администрирования Kaspersky Security Center, работающего локально.
- Устройства автоматически перемещаются в группу администрирования, указанную в параметрах инсталляционного пакета.

Задача удаленной установки в Kaspersky Security Center Cloud Console не может быть выполнена: нет целевых устройств, так как для всех устройств изменены параметры подключения. Вам нужно остановить задачу вручную после того, как убедитесь, что в столбце **Видимо в сети** списка управляемых устройств появился значок ошибки (!), для всех устройств из области переноса данных.

Перенос данных с виртуальными Серверами администрирования

Если у вас есть виртуальные Серверы администрирования в существующей инфраструктуре Kaspersky Security Center, вы не можете перенести данные из приложения Kaspersky Security Center, работающего локально, в Kaspersky Security Center Cloud Console с помощью мастера переноса данных. Также вы сможете выполнить перенос данных только для устройств ваших клиентов. Вам придется создать политики, задачи и отчеты вручную.

Вы можете выполнить один из следующих сценариев переноса данных:

- Переместив клиентские устройства с виртуальных Серверов администрирования на главный Сервер администрирования.
- Выполнив вручную перенос данных с виртуальных Серверов администрирования.

Сценарий: перенос данных с виртуальными Серверами администрирования с помощью перемещения устройств

Чтобы выполнить перенос данных из приложения Kaspersky Security Center Web Console, работающего локально, в Kaspersky Security Center Cloud Console, вы можете переместить свои устройства с виртуальных Серверов администрирования на главный Сервер администрирования.

Предварительные требования

Перед выполнением переноса данных вам нужно выполнить ряд действий, включая обновление Сервера администрирования, работающего локально, до версии 12 и выше и обновление управляемых приложений до версий, поддерживаемых приложением Kaspersky Security Center Cloud Console.

Сценарий переноса данных

Сценарий состоит из следующих этапов:

1. **Создание группы администрирования для каждого виртуального Сервера администрирования**

   Вы создаете группу в приложении Kaspersky Security Center, работающее локально.

2. **Переместите ваши клиентские устройства**

   Перемещение устройств клиентов с каждого виртуального Сервера администрирования в созданную на предыдущем этапе соответствующую группу администрирования, в приложении Kaspersky Security Center, работающем локально.

3. **Перенос данных**

   Выполните перенос данных, как описано для сети без иерархии виртуальных Серверов администрирования.

4. **Перемещение устройств под управление виртуальных Серверов администрирования (необязательный шаг)**

   Если вы хотите управлять своими клиентами с помощью виртуальных Серверов администрирования, переместите устройства из групп администрирования под управление виртуальных Серверов администрирования.

5. **Создание политик, задач и отчетов**

   Создайте требуемые политики, задачи и отчеты.

Результаты

После завершения переноса данных вы можете убедиться, что перенос данных прошел успешно:

- Агент администрирования перестановлен на всех управляемых устройствах.
- Все устройства управляются через Kaspersky Security Center Cloud Console.
- Все параметры объектов, действовавшие до переноса данных, сохранились.

Сценарий: перенос данных с виртуальными Серверами администрирования вручную

Вы можете выполнить перенос данных из приложения Kaspersky Security Center Web Console, работающего локально, в Kaspersky Security Center Cloud Console вручную.

Предварительные требования

Перед выполнением переноса данных вам нужно выполнить ряд действий, включая обновление Сервера администрирования, работающего локально, до версии 12 и выше и обновление управляемых приложений до версий, поддерживаемых приложением Kaspersky Security Center Cloud Console.

Сценарий переноса данных

Сценарий состоит из следующих этапов:

1. **Создание группы администрирования для каждого виртуального Сервера администрирования**

   Создайте группы администрирования, соответствующей каждому виртуальному Серверу администрирования, в Kaspersky Security Center Cloud Console.

2. **Создание автономного инсталляционного пакета Агента администрирования**

   Создайте автономный инсталляционный пакет Агента администрирования. Во время создания пакета укажите группу администрирования, созданную на предыдущем этапе. Вам нужно создать отдельный автономный инсталляционный пакет для каждой группы администрирования.

   Этот этап происходит в Kaspersky Security Center Cloud Console.

3. **Загрузка автономных инсталляционных пакетов**

   Загрузите автономные инсталляционные пакеты, которые вы создали на предыдущем этапе. Этот этап происходит в Kaspersky Security Center Cloud Console.

4. **Создание архива с каждым автономным инсталляционным пакетом**

   Доступные типы архивов: ZIP, CAB, TAR или TAR.GZ.

5. **Создание пользовательских инсталляционных пакетов Агента администрирования**

   Создайте пользовательские инсталляционные пакеты Агента администрирования. При создании используйте архивы, которые вы создали на предыдущем этапе.

   Этот этап выполняется в приложении Kaspersky Security Center, работающем локально.

6. **Создание задач удаленной установки**

   Создайте задачи удаленной установки приложений для установки Агента администрирования из созданных пользовательских инсталляционных пакетов.

   При создании задачи укажите соответствующую группу администрирования.

   Этот этап выполняется в приложении Kaspersky Security Center, работающем локально.

7. **Запуск созданных задач удаленной установки приложений**

   Агенты администрирования обновлены. Агенты администрирования переключаются под управление Сервера администрирования Kaspersky Security Center Cloud Console.

   Выполнен перенос данных в Kaspersky Security Center Cloud Console и все устройства помещаются в группы администрирования, которые были указаны при создании автономных инсталляционных пакетов Агента администрирования.

8. **Перемещение устройств под управление виртуальных Серверов администрирования (необязательный шаг)**

   Если вы хотите управлять своими клиентами с помощью виртуальных Серверов администрирования, переместите устройства из групп администрирования под управление виртуальных Серверов администрирования.

9. **Создание политик, задач и отчетов**

   Создайте требуемые политики, задачи и отчеты.

Результаты

После завершения переноса данных вы можете убедиться, что перенос данных прошел успешно:

- Агент администрирования перестановлен на всех управляемых устройствах.
- Все устройства управляются через Kaspersky Security Center Cloud Console.

  Все параметры объектов, действовавшие до переноса данных, сохранились.

Сценарий: перемещение устройств из групп администрирования под управление виртуальных Серверов

Вы можете управлять своими клиентами с помощью виртуальных Серверов администрирования. Если вы перенесли устройства и другие объекты из приложения Kaspersky Security Center, работающего локально, в Kaspersky Security Center Cloud Console, устройства будут размещены в группах администрирования. Для управления устройствами клиентов с помощью виртуальных Серверов администрирования необходимо переместить устройства из групп администрирования под управление виртуальных Серверов администрирования.

Предварительные требования

У вас есть созданный виртуальный Сервер администрирования для каждого из ваших клиентов.

Все устройства каждого клиента находятся в отдельной группе администрирования.

Этапы

Сценарий состоит из следующих этапов:

1. **Создание автономного инсталляционного пакета Агента администрирования**

   Переключитесь на каждый из созданных виртуальных Серверов администрирования, затем создайте автономный инсталляционный пакет для Агента администрирования. Вы можете переключать Серверы администрирования в главном меню, нажав на значок шеврона (›) справа от имени текущего Сервера администрирования и выбрав требуемый Сервер администрирования.

2. **Загрузка автономных инсталляционных пакетов**

   Загрузите автономные инсталляционные пакеты, которые вы создали на предыдущем этапе.

3. **Создание архива с каждым автономным инсталляционным пакетом**

   Доступные типы архивов: ZIP, CAB, TAR или TAR.GZ.

4. **Создание пользовательских инсталляционных пакетов Агента администрирования**

   Создайте пользовательские инсталляционные пакеты Агента администрирования. При создании используйте архивы, которые вы создали на предыдущем этапе.

   Этот этап происходит на главном Сервере администрирования.

5. **Создание задач удаленной установки**

   Создайте задачи удаленной установки приложений для установки Агента администрирования из созданных пользовательских инсталляционных пакетов.

   При создании задачи укажите соответствующую группу администрирования.

   Этот этап происходит на главном Сервере администрирования.

6. **Запуск созданных задач удаленной установки приложений**

   Агенты администрирования обновлены. Устройства переданы под управление виртуальных Серверов администрирования.

7. **Создание политик, задач и отчетов**

   Создайте требуемые политики, задачи и отчеты.

Результаты

Теперь вы можете управлять перенесенными устройствами клиентов с помощью виртуальных Серверов администрирования.

Выбор региона для доступа к Kaspersky Security Center Cloud Console

Каждая рабочая область размещается в определенном регионе развертывания в зависимости от страны или территории, указанной при создании рабочей области.

Когда вы входите в Kaspersky Security Center Cloud Console с помощью единого адреса `ksc.kaspersky.com`, ближайший к вам регион выбирается в соответствии с вашим IP-адресом. Это обеспечивает глобальное покрытие, доступность сервисов и эффективную работу решения.

Для использования решения Kaspersky SIEM Cloud подключение к Kaspersky Security Center Cloud Console должно выполняться через регион развертывания вашей рабочей области.

Это значит, что при подключении к рабочей области из другого региона необходимо использовать прямой адрес, соответствующий региону развертывания вашей рабочей области:

- Для Европы:

  ```
  ne.nwc.ksc.kaspersky.com
  ```

- Для Бразилии:

  ```
  bs.nwc.ksc.kaspersky.com
  ```

Решение Kaspersky SIEM Cloud недоступно в Мексике.

Мастер первоначальной настройки

В этом разделе представлена информация о работе мастера первоначальной настройки Сервера администрирования.

О мастере первоначальной настройки

Мастер первоначальной настройки в Kaspersky Security Center Cloud Console позволяет создать минимальный набор необходимых задач и политик, настроить минимальный набор параметров и приступить к созданию инсталляционных пакетов приложений "Лаборатории Касперского". Используя мастер, вы можете внести в Kaspersky Security Center Cloud Console следующие изменения:

- Инициировать загрузку инсталляционных пакетов для управляемых приложений "Лаборатории Касперского".
- Создать автономный инсталляционный пакет Агента администрирования для устройств под управлением Windows, Linux или macOS.
- Создать политику Агента администрирования Kaspersky Security Center.
- Создать задачу *Загрузка обновлений в хранилища точек распространения*.
- Создать политики и задачи для управляемых приложений "Лаборатории Касперского".
- Настроить взаимодействие с Kaspersky Security Network (KSN).

После завершения работы мастера первоначальной настройки инсталляционные пакеты Агента администрирования и управляемых приложений "Лаборатории Касперского" появляются в списке **Управление программным обеспечением → Инсталляционные пакеты**.

Мастер первоначальной настройки создает политики для управляемых приложений, таких как Kaspersky Endpoint Security для Windows, если такие политики не были созданы в группе Управляемые устройства. Мастер первоначальной настройки создает задачи, если задачи с такими же именами не были созданы в группе Управляемые устройства.

Kaspersky Security Center Cloud Console автоматически предлагает запустить мастер первоначальной настройки после создания рабочей области организации и первого запуска Kaspersky Security Center Cloud Console. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

Запуск мастера первоначальной настройки

Kaspersky Security Center Cloud Console автоматически предлагает запустить мастер первоначальной настройки после создания рабочей области организации и первого запуска Kaspersky Security Center Cloud Console. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

При повторном запуске мастера первоначальной настройки задачи и политики, созданные при предыдущем запуске мастера, не создаются повторно.

Чтобы запустить мастер первоначальной настройки вручную:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Общие**.

3. Перейдите по ссылке **Запустить мастер первоначальной настройки**.

Также можно запустить мастер первоначальной настройки, выбрав **Обнаружение устройств и развертывание → Развертывание и назначение → Мастер первоначальной настройки**.

Мастер предложит выполнить первоначальную настройку Kaspersky Security Center Cloud Console. Следуйте далее указаниям мастера. Для продолжения работы мастера нажмите на кнопку **Далее**. Используйте кнопку **Назад**, чтобы вернуться на предыдущий шаг мастера.

Шаг 1. Выбор инсталляционных пакетов для загрузки

В списке выберите приложения "Лаборатории Касперского" Kaspersky для установки на клиентские устройства. Kaspersky Security Center Cloud Console создаст инсталляционные пакеты для выбранных приложений. После этого вы будете использовать созданные инсталляционные пакеты для установки приложений.

При выборе инсталляционного пакета для загрузки обратите внимание на язык пакета: инсталляционные пакеты доступны на разных языках.

Выберите следующие приложения:

- Агент администрирования Kaspersky Security Center.

  При выборе инсталляционных пакетов Агента администрирования учитывайте следующее:

  - На каждом клиентском устройстве должен быть установлен Агент администрирования. Поэтому выберите Агент администрирования, подходящий для каждой операционной системы, установленной на клиентских устройствах.

  - Агент администрирования должен быть установлен вручную с помощью автономного инсталляционного пакета на устройстве, которое вы выбрали в качестве точки распространения. Точки распространения необходимы для опроса по сети и удаленной установки приложений безопасности "Лаборатории Касперского" на клиентские устройства. Поэтому необходимо выбрать хотя бы один инсталляционный пакет Агента администрирования. При переходе к следующим шагам мастера приложение Kaspersky Security Center Cloud Console создает автономный инсталляционный пакет Агента администрирования.

    По сравнению с точками распространения с операционной системой Windows, точки распространения с операционными системами Linux и macOS, имеют ограниченную функциональность. Рекомендуется выбирать компьютеры с операционной системой Windows в качестве точек распространения.

Вы можете выбрать Агенты администрирования для Windows, Linux и macOS. Если вы выберете Агент администрирования только для одной операционной системы, например, macOS, то для выбранной операционной системы будет создан автономный инсталляционный пакет. Если вы выберете Агент администрирования для нескольких операционных систем, Kaspersky Security Center Cloud Console создаст только один автономный инсталляционный пакет в соответствии со следующими приоритетами: Windows имеет самый высокий приоритет, далее Linux, а затем macOS. Например, если вы выберете Агенты администрирования для Linux и macOS, Kaspersky Security Center Cloud Console создаст автономный инсталляционный пакет Агента администрирования для Linux. Вы можете в любое время создать автономный инсталляционный пакет Агента администрирования для любой из этих операционных систем вручную.

- Приложения безопасности "Лаборатории Касперского".

  Выберите инсталляционные пакеты, соответствующие операционной системе, установленной на клиентских устройствах в вашей организации.

Шаг 2. Настройка параметров прокси-сервера

Если ваша организация использует прокси-сервер для подключения к интернету, укажите параметры прокси-сервера на этом шаге мастера. Эти параметры добавляются в инсталляционный пакет Агента администрирования. После установки Агент администрирования автоматически использует эти параметры на каждом клиентском устройстве.

Настройте следующие параметры подключения к прокси-серверу:

- **Использовать прокси-сервер**
- **Адрес**
- **Номер порта**
- **Аутентификация на прокси-сервере**

  Если этот параметр включен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

  По умолчанию параметр выключен.

- **Имя пользователя**

  Имя пользователя учетной записи, от имени которой будет выполняться подключение к прокси-серверу.

  Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

- **Пароль**

  Пароль учетной записи, от имени которой будет выполняться подключение к прокси-серверу.

  Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

Шаг 3. Настройка Kaspersky Security Network

Если на первом шаге мастера вы загрузили инсталляционный пакет Kaspersky Endpoint Security для Windows, отображается текст Положения о KSN для следующих приложений:

- Kaspersky Endpoint Security для Windows;
- приложение Kaspersky Security Center, установленное на локальных устройствах;
- приложение Kaspersky SIEM Cloud, установленное в облачном окружении.

Если вы не загрузили инсталляционный пакет Kaspersky Endpoint Security для Windows, Положение о KSN для этого приложения не отображается.

В пробной версии отображается только Положение о KSN для Kaspersky Endpoint Security для Windows.

Внимательно прочитайте условия Положения о Kaspersky Security Network. Выберите один из следующих вариантов:

- **Я принимаю условия использования Kaspersky Security Network**

  Kaspersky SIEM Cloud и управляемые приложения, установленные на клиентских устройствах, в автоматическом режиме будут предоставлять информацию об их работе Kaspersky Security Network. Сотрудничество с Kaspersky Security Network обеспечивает более быстрое обновление баз данных о вирусах и угрозах, что увеличивает скорость реагирования на возникающие угрозы безопасности.

- **Я не принимаю условия использования Kaspersky Security Network**

  Kaspersky SIEM Cloud и управляемые приложения не будут предоставлять информацию о своей работе Kaspersky Security Network.

  Если вы выбрали этот параметр, использование Kaspersky Security Network будет выключено.

По умолчанию использование KSN выключено. Если в дальнейшем вы измените мнение по поводу использования KSN, можете включить (или выключить) соответствующий параметр в окне свойств Сервера администрирования в разделе **Прокси-сервер KSN**.

Шаг 4. Настройка управления обновлениями приложений сторонних производителей

Этот шаг не отображается, если задача *Поиск уязвимостей и требуемых обновлений*.

Если вы хотите получать список обновлений для приложений, установленных на управляемых устройствах, а также список обнаруженных уязвимостей и рекомендуемых исправлений для них, то включите параметр **Поиск обновлений приложений сторонних производителей и исправлений для уязвимостей**. Если параметр включен, Kaspersky Security Center Cloud Console создает задачу *Поиск уязвимостей и требуемых обновлений*.

Шаг 5. Создание базовой конфигурации защиты сети

На этом шаге мастера нажмите на кнопку **Создать**, чтобы создать объекты, необходимые для начальной защиты ваших клиентских устройств.

Kaspersky Security Center Cloud Console выполняет две операции:

- Создание основных политик и задач с параметрами по умолчанию.

  Созданы следующие политики:

  - политика Агента администрирования Kaspersky Security Center;
  - политики управляемых приложений "Лаборатории Касперского".

  Созданы следующие задачи:

  - Задачи *Загрузка обновлений в хранилища точек распространения*.
  - задача *Поиск уязвимостей и требуемых обновлений*.

    Эта задача создается, только если вы включили параметр **Поиск обновлений приложений сторонних производителей и исправлений для уязвимостей** на предыдущем шаге мастера.
  - Задачи для управляемых приложений "Лаборатории Касперского".

- Создание автономного инсталляционного пакета Агента администрирования

  Вы будете использовать этот пакет для установки Агента администрирования на точках распространения. Kaspersky Security Center Cloud Console создает автономный инсталляционный пакет на основе инсталляционного пакета Агента администрирования, выбранного вами на предыдущем шаге мастера. Во время создания пакета вам нужно прочитать и принять условия Лицензионного соглашения для Агента администрирования. Когда автономный инсталляционный пакет создан, отобразится предложение загрузить его на устройство, которое вы используете в данный момент.

  На создание автономного инсталляционного пакета Агента администрирования может потребоваться некоторое время. Перейдите к следующему шагу мастера. Процесс будет продолжен в фоновом режиме. Вы можете отслеживать статус загрузки инсталляционного пакета, а также фильтровать и сортировать статусы в столбце **Статус инсталляционного пакета** (**Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**).

Каждый автономный инсталляционный пакет подписывается с помощью сертификата для аутентификации. Сертификат перевыпускается каждые три месяца. После каждого переиздания сертификата Kaspersky Security Center Cloud Console автоматически обновляет подписи всех созданных автономных инсталляционных пакетов. Для загруженных автономных инсталляционных пакетов обновление подписи не может выполняться автоматически. Поэтому когда срок действия сертификата истекает, при установке приложения из автономного инсталляционного пакета, может возникнуть ошибка сертификата. В этом случае загрузите автономный инсталляционный пакет еще раз.

Также срок действия сертификата можно посмотреть в свойствах файла автономного инсталляционного пакета, загруженного на ваше устройство. Для этого нажмите правой кнопкой мыши на автономном инсталляционном пакете и перейдите к его сведениям. На вкладке **Цифровые подписи** в списке выберите нужный сертификат и нажмите на кнопку **Сведения**, далее в открывшемся окне нажмите на кнопку **Просмотр сертификата**.

Шаг 6. Завершение работы мастера первоначальной настройки

На странице завершения работы мастера первоначальной настройки ознакомьтесь с дополнительными операциями, которые необходимо выполнить для развертывания приложений безопасности "Лаборатории Касперского" на клиентских устройствах. Выполните этапы, предусмотренные в сценарии первоначального развертывания приложений "Лаборатории Касперского".

Первоначальное развертывание приложений "Лаборатории Касперского"

В этом разделе описано первоначальное развертывание приложений "Лаборатории Касперского" на клиентских устройствах в вашей организации.

Сценарий: первоначальное развертывание приложений "Лаборатории Касперского"

В этом сценарии описана установка приложений "Лаборатории Касперского" на клиентские устройства в Kaspersky Security Center Cloud Console. Сначала вам нужно спланировать архитектуру решения с расчетом использования точек распространения, в том числе с ролью шлюза соединений. Далее вам нужно развернуть точки распространения в локальной сети и DMZ. Затем с помощью точек распространения в локальной сети вам нужно выполнить опрос сети и обнаружить сетевые устройства в вашей сети. После этого вы можете развернуть приложения "Лаборатории Касперского" на сетевых устройствах.

После завершения сценария приложения "Лаборатории Касперского" будут развернуты на выбранных клиентских устройствах в сети организации. Вы можете управлять всеми устройствами с установленными приложениями "Лаборатории Касперского".

Предварительные требования

Убедитесь, что выполнены следующие предварительные требования:

- Мастер первоначальной настройки завершен.
- Агент администрирования и инсталляционные пакеты приложения безопасности созданы.
- В соответствии с выбранной архитектурой решения настроены сетевые доступы к шлюзам соединений и прокси-серверу.
- Рассчитано необходимое количество точек распространения для каждого сегмента сети.
- Клиентские устройства в вашей организации не зашифрованы.

Этапы

Первоначальное развертывание приложений "Лаборатории Касперского" состоит из следующих этапов:

1. **Выбор устройств, которые выполняют роль точек распространения и шлюзов соединения**

   В Kaspersky Security Center Cloud Console точка распространения предназначена для:

   - опроса сети и обнаружения устройств;
   - удаленной установки Агента администрирования и средств защиты на клиентские устройства;
   - подключения клиентских устройств к Серверу администрирования (когда точка распространения выполняет роль шлюза соединения).

   Выберите устройства в сети вашей организации, которые выполняют роль точек распространения для группы администрирования. Выбранные устройства должны отвечать требованиям для точек распространения. В зависимости от количества клиентских устройств в сети вашей организации выберите требуемое количество устройств на роли точек распространения и шлюзов соединений.

   Если у вас много устройств, работающих вне сети организации, важно организовать шлюз соединений во внешней сети DMZ или облачного провайдера. Это сократит количество прямых подключений к Серверу администрирования.

   Начните развертывание решения с установки шлюзов соединений. Шлюзы соединений обеспечат подключение остальных клиентских устройств. Затем установите дополнительные точки распространения без роли шлюза соединений в сегментах сети для распределения нагрузки передаваемых данных.

2. **Создание автономного инсталляционного пакета Агента администрирования**

   Создайте автономный инсталляционный пакет Агента администрирования для установки на точку распространения. Не указывайте параметр шлюза соединения в параметрах данного пакета.

   Если клиентские устройства, выбранные для точек распространения, не имеют прямого доступа к Серверу администрирования через интернет, в параметрах инсталляционного пакета Агента администрирования настройте параметры прокси-сервера.

3. **Установка Агента администрирования на выбранное устройство, выполняющее роль точки распространения**

   Доставьте автономный инсталляционный пакет Агента администрирования на выбранное устройство любым способом. Например, вы можете скопировать автономный инсталляционный пакет на съемный диск (запоминающее устройство) или переместить его в папку общего доступа.

   В окне **Свойства** файла автономного инсталляционного пакета убедитесь, что автономный инсталляционный пакет для Агента администрирования подписан "Лабораторией Касперского".

   Запустите установку автономного инсталляционного пакета Агента администрирования на клиентском устройстве. Агент администрирования установлен с параметрами, указанными в инсталляционном пакете Агента администрирования, и подключен к Серверу администрирования. Устройство с Агентом администрирования перемещается в группу администрирования, которая была указана при создании автономного инсталляционного пакета для Агента администрирования.

4. **Назначение устройства с установленным Агентом администрирования точкой распространения**

   Назначьте устройства с установленным Агентом администрирования точкой распространения. Включите push-сервер на точке распространения для оперативного обмена данными. Если планируете подключать клиентские устройства через точку распространения, включите шлюз соединений. В разделе **Область действия** укажите область, на которую точка распространения распространяет обновления (группы администрирования и/или сетевое местоположение).

5. **Настройка и выполнение опроса сети точками распространения**

   Настройте опрос сети в соответствии со сценарием работы точки распространения с установленным Агентом администрирования. Вы также можете настроить опрос сети в политике Агента администрирования.

   После завершения опроса сети по расписанию клиентские устройства, подключенные к вашей сети организации, обнаружены и помещены в группу **Нераспределенные устройства**.

6. **Создание инсталляционных пакетов для Агента администрирования и управляемых приложений "Лаборатории Касперского"**

   Если вы не запускали мастер первоначальной настройки или пропустили этап создания инсталляционных пакетов, создайте инсталляционные пакеты для приложений "Лаборатории Касперского". Вам нужно создать оба инсталляционных пакета, для Агента администрирования и для управляемых приложений "Лаборатории Касперского", соответствующие операционной системе, установленной на клиентских устройствах в вашей организации.

7. **Удаление приложений безопасности сторонних производителей**

   Если на клиентских устройствах в сети вашей организации установлены приложения безопасности сторонних производителей, удалите их перед установкой приложений "Лаборатории Касперского".

8. **Установка приложений "Лаборатории Касперского" на клиентские устройства**

   Настройте политики управления защитой для конечных устройств в соответствиями с вашими требованиями.

   Для оптимальной работы с точками распространения в политике Агента администрирования включите следующие параметры:

   - Использовать шлюз соединения точки распространения (при наличии) в параметрах подключения по умолчанию.
   - Использовать точку распространения для принудительного подключения к Серверу.
   - Использовать UDP-порт.
   - Открывать порты Агента администрирования в брандмауэре Microsoft Windows.

   Создайте задачи для установки Агента администрирования и управляемых приложений "Лаборатории Касперского" на клиентские устройства в сети вашей организации. При создании задач используйте тип задачи **Удаленная установка приложения**. Для задачи установки Агента администрирования используйте параметр **Средствами операционной системы с помощью точек распространения**. Для задачи установки управляемых приложений "Лаборатории Касперского" используйте параметр **С помощью Агента администрирования**. После создания задач, вы можете настроить их параметры. Убедитесь, что расписание запуска каждой задачи соответствует вашим требованиям. Сначала должна быть запущена задача установки Агента администрирования. После установки Агента администрирования на клиентские устройства необходимо запустить задачу установки управляемых приложений "Лаборатории Касперского".

   Вы также можете создать одну задачу удаленной установки для установки Агента администрирования и управляемых приложений "Лаборатории Касперского" на клиентские устройства в сети вашей организации. В этом случае в блоке **Инсталляционные пакеты** используйте параметры **Выбор инсталляционного пакета** и **Выбор Агент администрирования**; в блоке **Принудительно скачать инсталляционный пакет** используйте параметр **Средствами операционной системы с помощью точек распространения**.

Вы можете создать несколько задач удаленной установки, чтобы установить управляемые приложения "Лаборатории Касперского" для различных групп администрирования или выборок устройств. Встроенные средства развертывания Kaspersky Security Center Cloud Console позволяют разворачивать Агент администрирования только с одной схемой подключения за раз. Если вы задействуете разные схемы подключения конечных устройств к Kaspersky Security Center Cloud Console, для автоматизации развертываний на постоянной основе мы рекомендуем задействовать внешние средства централизованного развертывания, например Windows Domain Group Policy, Microsoft System Center Configuration Manager, Microsoft Intune, Ansible или Puppet.

Для развертывания средствами Kaspersky Security Center Cloud Console последовательно выполните задачу установки Агента администрирования для списка устройств с одинаковыми настройками подключения к шлюзу соединений, прокси-сервера или прямым подключением к Kaspersky Security Center Cloud Console. По завершении установки измените параметры подключения в пакете Агента администрирования на необходимые для нового сегмента сети и переходите к развертыванию для следующего набора устройств.

Если у вас есть клиентские устройства, которые находятся вне сети с точкой распространения, например, ноутбуки автономных пользователей, вам нужно создать, настроить параметры подключения к шлюзу соединений (при наличии) или Серверу администрирования и доставить автономный инсталляционный пакет Агента администрирования на эти клиентские устройства любым способом. Установите автономный инсталляционный пакет Агента администрирования локально на эти клиентские устройства. Затем вы можете установить управляемые приложения "Лаборатории Касперского" на устройства этих автономных пользователей, следуя тем же инструкциям, что и для других устройств, обнаруженных точкой распространения.

Запустите задачи удаленной установки приложений.

Вы также можете запустить Мастер развертывания защиты, чтобы установить приложения "Лаборатории Касперского".

9. **Установка Kaspersky Security для мобильных устройств**

   Если вы планируете управлять корпоративными мобильными устройствами, см. справку Kaspersky Security для мобильных устройств информацию о развертывании Kaspersky Endpoint Security для Android.

10. **Проверка первоначального развертывания приложений "Лаборатории Касперского"**

    Сформируйте и просмотрите **Отчет о версиях приложений "Лаборатории Касперского"**. Убедитесь, что управляемые приложения "Лаборатории Касперского" установлены на всех клиентских устройствах в вашей организации.

Для полнодискового шифрования Kaspersky Security Center Cloud Console поддерживает только BitLocker.

Создание инсталляционных пакетов для приложений "Лаборатории Касперского"

Для развертывания приложений "Лаборатории Касперского" на сетевых устройствах вашей организации необходимо создать инсталляционные пакеты приложений "Лаборатории Касперского" в Kaspersky Security Center Cloud Console.

Чтобы создать инсталляционный пакет приложения "Лаборатории Касперского":

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Инсталляционные пакеты**. Вы также можете просматривать информацию о новых пакетах в списке экранных уведомлений. Если есть уведомления о новом пакете, вы можете перейти по ссылке рядом с уведомлением к списку доступных инсталляционных пакетов.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Выберите **Создать инсталляционный пакет для приложения "Лаборатории Касперского"**.

   Отобразится список дистрибутивов доступных на веб-серверах "Лаборатории Касперского". По умолчанию в списке отображаются только приложения на английском языке и на языке, соответствующим языку интерфейса. Чтобы отобразить другие языки, нажмите **Фильтр** и настройте параметры фильтра.

4. Выберите требуемый дистрибутив, например, **Kaspersky Endpoint Security для Windows (<номер версии>)**.

   Откроется окно с информацией о дистрибутиве.

5. Ознакомьтесь с информацией и нажмите на кнопку **Скачать и создать инсталляционный пакет**.

   Если дистрибутив не может быть автоматически преобразован в инсталляционный пакет, вместо кнопки **Скачать и создать инсталляционный пакет** отображается кнопка **Скачать дистрибутив**. В этом случае загрузите дистрибутив, а затем используйте загруженный файл для создания пользовательского инсталляционного пакета.

   Перед процессом загрузки или во время загрузки некоторых приложений "Лаборатории Касперского" отображается кнопка **Показать Лицензионное соглашение**. Если эта кнопка отображается:

   a. Нажмите на кнопку **Показать Лицензионное соглашение**, чтобы прочитать Лицензионные соглашения.

   b. В открывшейся панели прочтите Лицензионные соглашения, отображаемые на экране.

      Чтобы просмотреть данные, обрабатываемые приложениями "Лаборатории Касперского", для которых вы хотите создать инсталляционный пакет, нажмите **Просмотреть список данных**.

   c. Выберите Лицензионные соглашения и нажмите **Принять**.

   Загрузка продолжится после принятия Лицензионных соглашений. Если вы нажмете на кнопку **Отклонить**, загрузка прекратится.

   Вы можете закрыть окно мастера. В этом случае процесс скачивания продолжится в фоновом режиме. Вы можете отслеживать статус загрузки инсталляционного пакета, а также фильтровать и сортировать статусы в столбце **Статус инсталляционного пакета**.

   Если процесс загрузки останавливается и статус загрузки меняется на **Принять Лицензионное соглашение**, нажмите на имя инсталляционного пакета и выполните шаги 5.a и 5.b.

   По умолчанию инсталляционные пакеты со статусами **В процессе** и **Принять Лицензионное соглашение** располагаются в начале списка.

Если вы планируете выполнить перенос данных из Kaspersky Security Center Web Console в Kaspersky Security Center Cloud Console, использование прокси-сервера для доступа к корпоративной сети может повлиять на перенос данных. После того, как вы создадите инсталляционный пакет Агента администрирования, вам нужно указать параметры прокси-сервера, чтобы обеспечить соединение экземпляров Агента администрирования на управляемых устройствах с рабочей областью Kaspersky Security Center Cloud Console:

a. Нажмите на имя установочного пакета.

b. В открывшемся окне свойств инсталляционного пакета выберите вкладку **Параметры**.

c. Откройте раздел **Подключение**.

d. Выберите параметр **Использовать прокси-сервер** и заполните поля **Адрес прокси-сервера** и **Порт прокси-сервера**.

6. После завершения загрузки нажмите на кнопку **Закрыть** (✕), чтобы закрыть информационное окно дистрибутива.

Инсталляционный пакет создан. Инсталляционный пакет появится в списке инсталляционных пакетов.

Вы не можете добавить инсталляционный пакет с одним и тем же языком локализации несколько раз. Например, если вы уже добавили инсталляционный пакет Kaspersky Endpoint Security для Windows (английский), вы можете добавить инсталляционные пакеты Kaspersky Endpoint Security для Windows на других языках, кроме английского.

Распространение инсталляционных пакетов на подчиненные Серверы администрирования

Чтобы распространить инсталляционные пакеты на подчиненные Серверы администрирования:

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.

2. Запустите создание задачи распространения инсталляционного пакета на подчиненные Серверы администрирования одним из следующих способов:

   - Если вы хотите сформировать задачу для подчиненных Серверов выбранной группы администрирования, запустите создание групповой задачи для этой группы.

   - Если вы хотите сформировать задачу для набора подчиненных Серверов, запустите создание задачи для набора устройств.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

   В окне **Новая задача** мастера создания задачи, в поле **Тип задачи** выберите **Распространение инсталляционного пакета**. Вы также можете изменить имя задачи по умолчанию в поле **Название задачи**.

   На следующем шаге укажите подчиненные Серверы администрирования для области задачи и следуйте указаниям мастера создания задачи. В результате работы мастера создания задачи будет создана задача распространения выбранных инсталляционных пакетов на указанные подчиненные Серверы администрирования.

При создании задачи Распространение инсталляционного пакета для подчиненных Серверов администрирования, работающих локально, в область распространения, помимо пользовательских инсталляционных пакетов, будут включены только инсталляционные пакеты приложений "Лаборатории Касперского", которые поддерживаются приложением Kaspersky Security Center Web Console, работающим локально, – независимо от того, какой вариант распространения был выбран (**Все инсталляционные пакеты** или **Выбранные инсталляционные пакеты**).

3. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи выбранные инсталляционные пакеты будут скопированы на выбранные подчиненные Серверы администрирования.

Создание автономных инсталляционных пакетов Агента администрирования

Вы и пользователи устройств в вашей организации можете использовать автономные инсталляционные пакеты для локальной установки Агента администрирования на устройства. Автономный инсталляционный пакет может быть создан для устройств под управлением операционных систем Windows, Linux или macOS.

В Kaspersky Security Center Cloud Console вы можете создавать автономные инсталляционные пакеты только для Агента администрирования.

Автономный инсталляционный пакет представляет собой исполняемый файл, который можно отправить по почте или передать на клиентское устройство другим способом. Полученный файл можно запустить локально на клиентском устройстве, чтобы установить Агент администрирования без участия Kaspersky SIEM Cloud.

Для Агента администрирования для Linux и для Агента администрирования для macOS автономный инсталляционный пакет представляет собой файл сценария с расширением .sh. Когда вы запускаете этот файл сценария, выполняется распаковка вложенного архива, содержащего инсталляционный пакет и его параметры, а затем начинается установка.

Если Сервер администрирования имеет доступ в интернет, для загрузки зависимостей, необходимых для создания автономных инсталляционных пакетов Агента администрирования, используется задача **Загрузка обновлений в хранилище Сервера администрирования**. Если у Сервера администрирования нет доступа в интернет, выполните следующие действия:

1. Выполните следующую команду, чтобы создать флаг RIUtilsArchiveDirUsed:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Выполните следующую команду, чтобы перезапустить службу Сервера администрирования:

   ```
   systemctl restart kladminserver_srv.service
   ```

Загрузите следующие архивы с сайта "Лаборатории Касперского" и поместите их в директорию /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives:

- ri_utils_win32.zip
- ri_utils_arm64.zip

Не переименовывайте архивы.

Теперь у Сервера администрирования есть нужные зависимости.

Если вы устанавливаете Агент администрирования с помощью автономного инсталляционного пакета на устройство под управлением 32-разрядной версии Microsoft Windows XP Professional for Embedded Systems, установка завершится неудачно. Чтобы избежать этого, предварительно установите обновление KB2868626 для Windows XP, загрузив его с веб-сайта Microsoft: https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626.

Каждый автономный инсталляционный пакет подписывается с помощью сертификата для аутентификации. Сертификат перевыпускается каждые три месяца. После каждого переиздания сертификата Kaspersky Security Center Cloud Console автоматически обновляет подписи всех созданных автономных инсталляционных пакетов. Для загруженных автономных инсталляционных пакетов обновление подписи не может выполняться автоматически. Поэтому когда срок действия сертификата истекает, при установке приложения из автономного инсталляционного пакета, может возникнуть ошибка сертификата. В этом случае загрузите автономный инсталляционный пакет еще раз.

Также срок действия сертификата можно посмотреть в свойствах файла автономного инсталляционного пакета, загруженного на ваше устройство. Для этого нажмите правой кнопкой мыши на автономном инсталляционном пакете и перейдите к его сведениям. На вкладке **Цифровые подписи** в списке выберите нужный сертификат и нажмите на кнопку **Сведения**, далее в открывшемся окне нажмите на кнопку **Просмотр сертификата**.

Чтобы создать автономный инсталляционный пакет:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов. Если инсталляционный пакет Агента администрирования отсутствует в списке, создайте этот инсталляционный пакет вручную.

2. В списке инсталляционных пакетов, нажмите на имя инсталляционного пакета Агента администрирования.

   Отобразится окно свойств инсталляционного пакета Агента администрирования.

3. При необходимости настройте параметры инсталляционного пакета Агента администрирования и закройте окно свойств инсталляционного пакета Агента администрирования.

4. В списке инсталляционных пакетов выберите пакет и над списком нажмите на кнопку **Развернуть**.

5. Выберите параметр **С использованием автономного инсталляционного пакета**.

   Запустится мастер создания автономного инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

6. Убедитесь, что включен параметр **Установить Агент администрирования совместно с данным приложением**, если требуется установить Агент администрирования совместно с выбранным приложением.

Параметр отображается в зависимости от приложения, для которого вы создаете автономный инсталляционный пакет.

По умолчанию параметр включен. Рекомендуется включить этот параметр, если вы не уверены, установлен ли на устройстве Агент администрирования. Если Агент администрирования уже установлен на устройстве, после установки автономного инсталляционного пакета с Агентом администрирования, Агент администрирования будет обновлен до более новой версии.

Если вы выключите этот параметр, Агент администрирования не будет установлен на устройство, и устройство не будет управляемым.

Если автономный инсталляционный пакет для выбранного приложения уже существует на Сервере администрирования, мастер отобразит сообщение об этом. В этом случае вам нужно выбрать одно из следующих действий:

- **Создать автономный инсталляционный пакет**. Выберите этот параметр, например, если вы хотите создать автономный инсталляционный пакет для новой версии приложения, и чтобы также остался автономный инсталляционный пакет для предыдущей версии приложения, который вы создали ранее. Новый автономный инсталляционный пакет расположен в другой папке.

- **Использовать существующий автономный инсталляционный пакет**. Выберите этот параметр, если вы хотите использовать существующий автономный инсталляционный пакет. Процесс создания пакета не запускается.

- **Сформировать заново существующий автономный инсталляционный пакет**. Выберите этот параметр, если хотите создать автономный инсталляционный пакет для этого же приложения еще раз. Автономный инсталляционный пакет размещается в той же папке.

7. На шаге **Перемещение в список управляемых устройств** параметр **Не перемещать устройства** выбран по умолчанию. Если вы не хотите перемещать клиентское устройство ни в какую группу администрирования после установки Агента администрирования, не изменяйте этот параметр.

   Если вы хотите переместить клиентское устройство после установки Агента администрирования, выберите параметр **Перемещать нераспределенные устройства в эту группу** и укажите группу администрирования, в которую вы хотите переместить клиентское устройство. По умолчанию устройства перемещаются в группу **Управляемые устройства**.

8. Выберите параметр **Открыть список автономных пакетов**, если вы хотите, чтобы список автономных инсталляционных пакетов отображался после завершения работы мастера.

9. Нажмите на кнопку **Готово**.

   Мастер создания автономного инсталляционного пакета закрывается.

Автономный инсталляционный пакет Агента администрирования создан. Созданный автономный инсталляционный пакет отображается в списке автономных инсталляционных пакетов, которые вы можете просмотреть.

Просмотр списка автономных инсталляционных пакетов

Вы можете просмотреть список автономных инсталляционных пакетов и свойства каждого отдельного инсталляционного пакета.

Чтобы просмотреть список автономных инсталляционных пакетов для всех инсталляционных пакетов:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов.

2. Нажмите на кнопку **Просмотреть список автономных пакетов**.

Отобразится список автономных инсталляционных пакетов.

Свойства автономных инсталляционных пакетов в списке отображаются следующим образом:

- **Имя пакета**. Имя автономного инсталляционного пакета, которое автоматически формируется из имени и версии приложения, включенной в пакет.
- **Имя инсталляционного пакета Агента администрирования**.
- **Версия Агента администрирования**.
- **Размер**. Размер файла в мегабайтах (МБ).
- **Группа**. Имя группы, в которую перемещается клиентское устройство после установки Агента администрирования.
- **Создан**. Дата и время создания автономного инсталляционного пакета.
- **Изменен**. Дата и время изменения автономного инсталляционного пакета.
- **Хеш файла**. Это свойство используется для подтверждения того, что автономный инсталляционный пакет не был изменен сторонними лицами и у пользователя есть тот же файл, который вы создали и передали ему.

Чтобы просмотреть список автономных инсталляционных пакетов для определенного инсталляционного пакета,

выберите инсталляционный пакет в списке и над списком нажмите на кнопку **Просмотреть список автономных пакетов**.

В списке автономных инсталляционных пакетов вы можете сделать следующее:

- Удалить автономный инсталляционный пакет, нажав на кнопку **Удалить**.
- Загрузить автономный инсталляционный пакет на свое устройство, нажав на кнопку **Скачать**.

  Каждый автономный инсталляционный пакет подписывается с помощью сертификата для аутентификации. Сертификат перевыпускается каждые три месяца. После каждого переиздания сертификата Kaspersky Security Center Cloud Console автоматически обновляет подписи всех созданных автономных инсталляционных пакетов. Для загруженных автономных инсталляционных пакетов обновление подписи не может выполняться автоматически. Поэтому когда срок действия сертификата истекает, при установке приложения из автономного инсталляционного пакета, может возникнуть ошибка сертификата. В этом случае загрузите автономный инсталляционный пакет еще раз.

  Также срок действия сертификата можно посмотреть в свойствах загруженного автономного инсталляционного пакета. Для этого на вкладке **Цифровые подписи** в списке выберите нужный сертификат и нажмите на кнопку **Сведения**, далее в открывшемся окне нажмите на кнопку **Просмотр сертификата**.

Создание пользовательского инсталляционного пакета

Вы можете использовать пользовательские инсталляционные пакеты, чтобы:

- установить любое приложение (например, текстовый редактор) на клиентские устройства с использованием Kaspersky SIEM Cloud, например, с помощью задачи;
- создать автономный инсталляционный пакет.

Пользовательский инсталляционный пакет – это папка с набором файлов, включающая исполняемый файл. Источником для создания пользовательского инсталляционного пакета является архивный файл. Архивный файл содержит файл или файлы, которые должны быть включены в пользовательский инсталляционный пакет. Создавая пользовательский инсталляционный пакет, вы можете указать параметры командной строки, например для установки приложения в тихом режиме.

Вы не можете создать пользовательский инсталляционный пакет в пробном режиме Kaspersky SIEM Cloud.

Чтобы создать пользовательский инсталляционный пакет:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Выберите **Создать инсталляционный пакет из файла**.

4. Укажите имя инсталляционного пакета и нажмите на кнопку **Обзор**.

   В стандартном окне **Открыть** можно выбрать архивный файл для создания инсталляционного пакета.

5. Выберите архивный файл, расположенный на доступных дисках.

   Вы можете загрузить архивный файл формата ZIP, CAB, TAR или TAR.GZ. Создать инсталляционный пакет из файла формата SFX (самораспаковывающийся архив) нельзя.

   Файлы загружены на Сервер администрирования Kaspersky SIEM Cloud.

   Если Сервер администрирования обнаружит, что в архив входит приложение "Лаборатории Касперского", отобразится сообщение об ошибке. Вы можете загрузить инсталляционные пакеты приложений "Лаборатории Касперского" с веб-серверов "Лаборатории Касперского". Эта операция доступна, если выбрать **Управление программным обеспечением → Приложения "Лаборатории Касперского" → Каталог приложений "Лаборатории Касперского"**.

6. Если выбранный архивный файл включает в себя несколько исполняемых файлов, выберите один исполняемый файл, который необходимо запустить для установки приложения с использованием созданного инсталляционного пакета.

7. Если хотите, вы можете указать исполняемый файл в параметрах командной строки.

Вы можете указать параметры командной строки для установки приложения из инсталляционного пакета в тихом режиме. Дополнительную информацию о параметрах командной строки см. в документации производителя.

Начнется создание инсталляционного пакета.

В окне мастера отобразится информация о завершении процесса.

Если инсталляционный пакет не создан, отобразится сообщение об ошибке.

В Kaspersky Security Center Cloud Console общий размер всех пользовательских инсталляционных пакетов на Сервере администрирования ограничен 500 МБ. Если этот предел превышен при создании нового пользовательского инсталляционного пакета, удалите более старые пользовательские инсталляционные пакеты, созданные ранее. Размер инсталляционного пакета отображается в его свойствах.

8. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

Созданный пользовательский инсталляционный пакет будет загружен на Сервер администрирования. После загрузки инсталляционный пакет появится в списке инсталляционных пакетов.

В списке инсталляционных пакетов вы можете просмотреть следующие свойства пользовательского инсталляционного пакета:

- **Имя**. Название инсталляционного пакета.
- **Статус инсталляционного пакета**. Статус скачивания инсталляционного пакета.
- **Источник**. Имя поставщика приложения.
- **Приложение**. Название приложения, упакованного в пользовательский инсталляционный пакет.
- **Версия**. Версия приложения.
- **Язык**. Язык приложения, упакованного в пользовательский инсталляционный пакет.
- **Размер (МБ)**. Размер пользовательского инсталляционного пакета.
- **ОС**. Операционная система, для которой создается пользовательский инсталляционный пакет.
- **Создано**. Дата создания инсталляционного пакета.
- **Изменено**. Дата изменения инсталляционного пакета.
- **Тип**. Приложение "Лаборатории Касперского" или приложение стороннего производителя.

Нажав на имя пользовательского инсталляционного пакета в списке инсталляционных пакетов, вы можете изменить параметры командной строки и имя пользовательского инсталляционного пакета.

Требования для точки распространения

Чтобы обрабатывать до 10 000 клиентских устройств, точка распространения должна отвечать следующим минимальным требованиям (предоставлена конфигурация тестового стенда):

- Процессор: Intel® Core™ i7-7700 CPU, 3,60 ГГц, 4 ядра.
- Оперативная память: 8 ГБ.
- Свободное место на диске: 120 ГБ.

Кроме того, точка распространения должна иметь доступ в интернет и должна быть всегда подключена.

При наличии на Сервере администрирования задач удаленной установки, на устройстве с точкой распространения дополнительно потребуется дисковое пространство, равное суммарному размеру устанавливаемых инсталляционных пакетов.

При наличии на Сервере администрирования одного или нескольких экземпляров задачи установки обновлений (патчей) и закрытия уязвимостей на устройстве с точкой распространения дополнительно потребуется дисковое пространство, равное удвоенному суммарному размеру всех устанавливаемых патчей.

Вы можете включить обнаружение устройств для IPv4-диапазонов и IPv6-сетей. Параметр **Использовать Zeroconf для опроса IPv6-сетей** доступен в следующих случаях:

- Точка распространения работает под управлением Linux.
- Установлена утилита avahi-browse на точке распространения.

Для улучшения стабильности соединения рекомендуется настроить параметры keepalive на устройствах шлюза соединения.

Параметры инсталляционного пакета Агента администрирования

Чтобы настроить параметры инсталляционного пакета Агента администрирования:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Перейдите по ссылке с названием инсталляционного пакета Агента администрирования.

Отобразится окно свойств инсталляционного пакета Агента администрирования. Информация в окне сгруппирована по вкладкам и разделам.

Общие

Раздел **Общие** содержит общую информацию об инсталляционном пакете:

- название инсталляционного пакета;
- имя и версию приложения, для которого сформирован инсталляционный пакет;
- размер инсталляционного пакета;
- дата создания инсталляционного пакета;
- путь к папке размещения инсталляционного пакета.

Параметры

В этом разделе можно настроить параметры, необходимые для обеспечения работоспособности Агента администрирования сразу после его установки. Параметры этого раздела доступны только для устройств под управлением Windows.

В блоке параметров **Папка назначения** можно выбрать папку на клиентском устройстве, в которую будет установлен Агент администрирования.

- **Устанавливать в папку по умолчанию**

  Если выбран этот вариант, Агент администрирования будет установлен в папку <Диск>:\Program Files\Kaspersky Lab\NetworkAgent. Если такой папки нет, она будет создана автоматически.

  По умолчанию выбран этот вариант.

- **Устанавливать в заданную папку**

  Если выбран этот вариант, Агент администрирования будет установлен в папку, указанную в поле ввода.

В блоке параметров ниже можно задать пароль для задачи удаленной деинсталляции Агента администрирования:

- **Использовать пароль деинсталляции**

  Если параметр включен, можно ввести пароль для удаления приложения (доступно только для Агента администрирования на устройствах под управлением операционных систем семейства Windows).

  По умолчанию параметр выключен.

- **Статус**

- **Защитить службу Агента администрирования от неавторизованного удаления, остановки или изменения параметров работы**

  Если этот параметр включен, после того, как Агент администрирования был установлен на управляемом устройстве, компонент не может быть удален или изменен без требуемых прав. Работа Агента администрирования не может быть остановлена. Этот параметр не влияет на контроллеры домена.

Включите этот параметр, чтобы защитить Агент администрирования на рабочих станциях, управляемых с правами локального администратора.

По умолчанию параметр выключен.

- **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**

  Если этот параметр включен, все загруженные обновления и патчи для Сервера администрирования, Агента администрирования, OSMP Console и Сервера iOS MDM будут установлены автоматически.

  Если этот параметр выключен, то загруженные обновления и патчи будут установлены только после того, как вы измените их статус на *Одобрено*. Обновления и патчи со статусом *Не определено* не будут установлены.

  По умолчанию параметр включен.

Подключение

В этом разделе можно настроить параметры подключения Агента администрирования к Серверу администрирования:

- **Использовать UDP-порт**

  Номер UDP-порта

  В поле можно указать номер порта подключения Сервера администрирования к Агенту администрирования по протоколу UDP.

  По умолчанию номер UDP-порта – 15000.

- **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**

  Если параметр включен, порты, используемые Агентом администрирования, будут добавлены в список исключений брандмауэра Microsoft Windows.

  По умолчанию параметр включен.

- **Не использовать прокси-сервер**

- **Использовать прокси-сервер**

  Если этот параметр включен, для подключения Агента администрирования к Серверу администрирования и шлюзу соединений используется интернет-прокси-сервер.

  Адрес прокси-сервера

  Порт прокси-сервера

- **Аутентификация на прокси-сервере**

  Если этот параметр включен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

  По умолчанию параметр выключен.

  Имя пользователя

  Имя пользователя учетной записи, от имени которой будет выполняться подключение к прокси-серверу.

Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

Пароль

Пароль учетной записи, от имени которой будет выполняться подключение к прокси-серверу.

Рекомендуется указывать данные учетной записи с минимальными правами, необходимыми только для аутентификации на прокси-сервере.

В целях совместимости не рекомендуется указывать параметры подключения к прокси-серверу в параметрах инсталляционного пакета Агента администрирования.

Дополнительно

В этом разделе вы можете настроить способ использования шлюза соединения и виртуальной машины, а также указать регистрировать ли пользователя в качестве владельца устройства:

- **Подключаться к Серверу администрирования через шлюз соединения**

  Поддерживается только прямое подключение к шлюзу соединения. Параметр использования интернет-прокси-сервера, указанный в инсталляционном пакете, не применяется.

- **Адрес шлюза соединения**

- **Включить динамический режим для VDI**

  Если параметр включен, для Агента администрирования, установленного на виртуальной машине, будет включен динамический режим для Virtual Desktop Infrastructure (VDI).

  По умолчанию параметр выключен.

- **Оптимизировать параметры для VDI**

  Если параметр включен, в параметрах Агента администрирования выключены следующие функции:

  - получение информации об установленном программном обеспечении;
  - получение информации об аппаратном обеспечении;
  - получение информации о наличии уязвимостей;
  - получение информации о необходимых обновлениях.

  По умолчанию параметр выключен.

- **Разрешить запуск утилиты регистрации пользователя после установки Агента администрирования**

  Если этот параметр включен, после установки Агента администрирования будет запущена утилита регистрации пользователя в качестве владельца устройства. По умолчанию параметр выключен.

Дополнительные компоненты

В этом разделе можно выбрать дополнительные компоненты для совместной установки с Агентом администрирования.

Теги

В разделе **Теги** отображается список ключевых слов (тегов), которые можно добавлять клиентским устройствам после установки на них Агента администрирования. Вы можете добавлять и удалять теги из списка, а также переименовывать теги.

Если рядом с тегом установлен флажок, тег будет автоматически добавлен управляемым устройствам при установке на них Агента администрирования.

Если флажок рядом с тегом снят, тег не будет автоматически добавлен управляемым устройствам при установке на них Агента администрирования. Этот тег можно добавить устройствам вручную.

При удалении тега из списка тег автоматически снимается со всех устройств, которым он добавлен.

История ревизий

В этом разделе можно посмотреть историю ревизий инсталляционного пакета. Вы можете сравнивать ревизии, просматривать ревизии, сохранять ревизии в файл, добавлять и изменять описания ревизий.

Параметры инсталляционного пакета Агента администрирования доступны для конкретной операционной системы, которые приведены в таблице ниже.

Параметры инсталляционного пакета Агента администрирования

Раздел свойств	Windows	Mac	Linux
Общие	✓	✓	✓
Параметры	✓	—	—
Подключение	✓	✓ * кроме флажка **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**	✓ * кроме флажка **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**
Дополнительно	✓	✓	✓
Дополнительные компоненты	✓	✓	✓
Теги	✓	✓ * кроме правил автоматического назначения тегов	✓ * кроме правил автоматического назначения тегов
История ревизий	✓	✓	✓

Виртуальная инфраструктура

Kaspersky SIEM Cloud поддерживает работу с виртуальными машинами. Для защиты виртуальной инфраструктуры вам нужно установить Агент администрирования на каждую виртуальную машину.

Рекомендации по снижению нагрузки на виртуальные машины

В случае инсталляции Агента администрирования на виртуальную машину следует рассмотреть возможность отключения той части функциональности Kaspersky SIEM Cloud, которая не очень полезна для виртуальных машин.

При установке Агента администрирования на виртуальную машину или на шаблон, из которого в дальнейшем будут получены виртуальные машины, рекомендуется выполнить следующие действия:

- если выполняется удаленная установка, в окне свойств инсталляционного пакета Агента администрирования (в разделе **Дополнительно**) выбрать параметр **Оптимизировать параметры для VDI**;
- если выполняется интерактивная установка с помощью мастера, в окне мастера выбрать параметр **Оптимизировать параметры Агента администрирования для виртуальной инфраструктуры**.

Выбор параметров изменит параметры Агента администрирования таким образом, чтобы по умолчанию (до применения политики) были выключены следующие функции:

- получение информации об установленном программном обеспечении;
- получение информации об аппаратном обеспечении;
- получение информации о наличии уязвимостей;
- получение информации о необходимых обновлениях.

Как правило, перечисленные функции не нужны на виртуальных машинах в силу того, что программное обеспечение и виртуальное аппаратное обеспечение на них единообразны.

Выключение функций обратимо. Если любая из выключенных функций все же нужна, ее можно включить при помощи политики Агента администрирования, или в локальных параметрах Агента администрирования. Локальные параметры Агента администрирования доступны из контекстного меню соответствующего устройства в Консоли администрирования.

Поддержка динамических виртуальных машин

Kaspersky SIEM Cloud поддерживает динамические виртуальные машины. Если в сети организации развернута виртуальная инфраструктура, то в некоторых случаях могут использоваться динамические (временные) виртуальные машины. Такие машины создаются с уникальными именами из заранее подготовленного администратором шаблона. Пользователь работает с созданной машиной некоторое время, а после выключения виртуальная машина удаляется из виртуальной инфраструктуры. Динамическая виртуальная машина, с установленным Агентом администрирования, также добавляется в базу данных Сервера администрирования. После выключения этой виртуальной машины запись о ней должна быть также удалена и из базы данных Сервера администрирования.

Чтобы функциональность автоматического удаления записей о виртуальных машинах работала, при установке Агента администрирования на шаблон, из которого будут созданы динамические виртуальные машины, нужно выбрать параметр **Включить динамический режим для VDI**:

- в случае удаленной установки – в окне свойств инсталляционного пакета Агента администрирования (раздел **Дополнительно**);
- в случае интерактивной установки – в мастере установки Агента администрирования.

Параметр **Включить динамический режим для VDI** не следует выбирать при установке Агента администрирования на физические устройства.

Если нужно, чтобы события с динамических виртуальных машин сохранялись на Сервере администрирования некоторое время после удаления машин, то следует в окне свойств Сервера администрирования в разделе **Хранилище событий** выбрать параметр **Хранить события после удаления устройств** и указать максимальное время хранения событий в днях.

Не рекомендуется включать шифрование дисков на динамических виртуальных машинах.

Поддержка копирования виртуальных машин

Kaspersky SIEM Cloud поддерживает копирование виртуальной машины с установленным Агентом администрирования или создание виртуальной машины из шаблона с установленным Агентом администрирования.

Агент администрирования может автоматически обнаруживать копирование виртуальных машин в следующих случаях:

- При установке Агента администрирования был выбран параметр **Включить динамический режим для VDI**: после каждой перезагрузки операционной системы такая виртуальная машина будет считаться новым устройством, независимо от факта ее копирования.
- Используется один из следующих гипервизоров: VMware™, HyperV® или Xen®: Агент администрирования определит факт копирования виртуальной машины по изменившимся идентификаторам виртуального аппаратного обеспечения.

Анализ изменений виртуального аппаратного обеспечения не абсолютно надежен. Прежде чем широко использовать данный метод, следует предварительно проверить его работоспособность на небольшом количестве виртуальных машин для используемой в организации версии гипервизора.

Использование Агента администрирования для Windows, Linux и macOS: сравнение

Агент администрирования для macOS и Linux имеет несколько функциональных ограничений по сравнению с Агентом администрирования для Windows. Свойства политики Агента администрирования и инсталляционного пакета зависят от операционной системы. В таблице ниже сравниваются возможности и сценарии использования Агента администрирования, доступные для операционных систем Windows, macOS и Linux.

Сравнение функций Агента администрирования

Функция Агента администрирования	Windows	Linux	macOS
Установка			
Автоматическая установка обновлений и патчей для Агента администрирования	✓	✓	–
Автоматическое распространение ключа	✓	✓	✓
Установка вручную с помощью запуска инсталляторов приложений на устройствах	✓	✓	✓
Принудительная синхронизация	✓	✓	✓ За исключением push-сервера
Точка распространения			
Опрос сети	✓ • Опрос IP-диапазонов • Опрос сети Windows • Опрос контроллеров домена (Microsoft Active Directory)	✓ • Опрос IP-диапазонов • Опрос контроллеров домена (Microsoft Active Directory, Samba как Active Directory, FreeIPA, ALD Pro)	–
Запуск службы прокси-сервер KSN на стороне точки распространения	✓	✓	–
Загрузка обновлений через серверы обновлений "Лаборатории Касперского" в хранилища точек распространения, которые распространяют обновления на управляемые устройства	✓	✓	– Точки распространения под управлением macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского". Если устройства с операционной системой macOS находятся в области действия задачи *Загрузка обновлений в хранилища точек распространения*, задача завершится со статусом *Сбой*, даже если она успешно завершилась на всех устройствах с операционной системой Windows.

Функция Агента администрирования	Windows	Linux	macOS
Принудительная установка приложений	✓	С ограничением: невозможно выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой Linux.	С ограничением: невозможно выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой macOS.
Работа с приложениями сторонних производителей			
Удаленная установка приложений на устройства	✓	—	—
Обновления программного обеспечения	✓	—	—
Настройка обновлений операционной системы в политике Агента администрирования	✓	—	—
Просмотр информации об уязвимостях в приложениях	✓	—	—
Поиск уязвимостей в приложениях	✓	—	—
Инвентаризация программного обеспечения, установленного на устройствах	✓	✓	—
Виртуальные машины			
Установка Агента администрирования на виртуальные машины	✓	✓	✓
Оптимизация параметров для VDI	✓	✓	✓
Поддержка динамических виртуальных машин	✓	✓	✓
Другое			
Аудит действий на удаленном клиентском устройстве с помощью совместного доступа к рабочему столу Windows	✓	—	—
Управление перезагрузкой устройств	✓	—	—
Менеджер соединений	✓	✓	✓
Профили соединения для автономных пользователей	✓	✓	✓
Удаленное подключение к рабочему столу клиентского устройства	✓	✓	✓

Следующие разделы отображаются в свойствах точки распространения, хотя соответствующие функции не поддерживаются Агентом администрирования для macOS:

- Источник обновлений
- Прокси-сервер KSN
- Windows-домены

- Active Directory
- IP-диапазоны
- Дополнительно
- Статистика

Указание параметров удаленной установки на устройствах под управлением Unix

Когда вы устанавливаете приложение на устройство под управлением Unix с помощью задачи удаленной установки, вы можете указать параметры, специфичные для Unix, для этой задачи. Эти параметры доступны в свойствах задачи после ее создания.

Чтобы указать параметры, специфичные для Unix, для задачи удаленной установки:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на имя задачи удаленной установки, для которой вы хотите указать параметры, специфичные для Unix.

   Откроется окно свойств задачи.
3. Перейдите в раздел **Параметры приложения** → **Параметры, специфичные для Unix**.
4. Задайте следующие параметры:

   - **Установить пароль для учетной записи root (только для развертывания через SSH)**

     Если команду `sudo` невозможно использовать на целевом устройстве без указания пароля, выберите этот параметр, а затем укажите пароль для учетной записи root. Kaspersky Next XDR Expert передает пароль в зашифрованном виде на целевое устройство, расшифровывает пароль, а затем запускает процедуру установки от имени учетной записи root с указанным паролем.

     > Kaspersky Next XDR Expert не использует учетную запись или указанный пароль для создания SSH-соединения.

   - **Укажите путь к временной папке с правами Выполнение на целевом устройстве (только для развертывания через SSH)**

     Если папка /tmp на целевом устройстве не имеет права Выполнение, выберите этот параметр, а затем укажите путь к папке с правами Выполнение. Kaspersky Next XDR Expert использует указанную папку в качестве временной папки для доступа по SSH. Приложение помещает инсталляционный пакет в директорию и запускает процедуру установки.
5. Нажмите на кнопку **Сохранить**.

Указанные параметры задачи сохранены.

Замещение приложений безопасности сторонних производителей

Для установки приложений безопасности "Лаборатории Касперского" средствами Kaspersky SIEM Cloud может потребоваться удалить стороннее программное обеспечение, несовместимое с устанавливаемым приложением. Open Single Management Platform предоставляет несколько способов удаления приложений сторонних производителей.

Удаление несовместимых приложений при настройке удаленной установки приложения

Вы можете включить параметр **Удалять несовместимые приложения автоматически** во время настройки удаленной установки приложения безопасности. Вы можете найти этот параметр в мастере развертывания защиты. Если этот параметр включен, Open Single Management Platform удаляет несовместимые приложения перед установкой приложения безопасности на управляемое устройство.

Удаление несовместимых приложений с помощью отдельной задачи

Для удаления несовместимых приложений используется задача **Удаленная деинсталляция приложения**. Задачу следует запускать на устройствах перед задачей установки приложения безопасности. Например, в задаче установки можно выбрать расписание типа **По завершении другой задачи**, где другой задачей является задача **Удаленная деинсталляция приложения**.

Этот способ удаления целесообразно использовать в случаях, если инсталлятор приложения безопасности не может успешно удалить какое-либо из несовместимых приложений.

Возможности ручной установки приложений

Вы можете установить Агент администрирования на устройства локально, не используя Kaspersky Security Center Cloud Console. Для этого создайте автономный инсталляционный пакет для Агента администрирования, как описано в следующем разделе: Создание автономного инсталляционного пакета. Перенесите пакет на клиентское устройство и установите его. После завершения установки Агента администрирования вы можете использовать устройство в качестве точки распространения.

Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky SIEM Cloud

Для того чтобы выполнить первоначальное развертывание Агента администрирования или других приложений, вы можете принудительно установить выбранные инсталляционные пакеты с помощью задачи удаленной установки Kaspersky SIEM Cloud при условии, что на каждом устройстве есть учетные записи пользователей с правами локального администратора.

В случае первоначального развертывания Агент администрирования не устанавливается. Поэтому в параметрах задачи удаленной установки невозможно выбрать распространение файлов, необходимых для установки приложения с помощью Агента администрирования. Вы можете распространять файлы, только используя ресурсы операционной системы с помощью точек распространения.

Вам нужно указать учетную запись, имеющую доступ к административным ресурсам общего доступа admin$, в параметрах задачи удаленной установки.

Вы можете указать целевые устройства явно (списком), выбрав группу администрирования Kaspersky SIEM Cloud, которой они принадлежат, либо созданием выборки устройств по определенному условию. Время запуска установки определяется расписанием задачи. Если в свойствах задачи включен параметр **Запускать пропущенные задачи**, задача может запускаться сразу при включении устройств или при переносе их в целевую группу администрирования.

Принудительная установка осуществляется путем доставки инсталляционных пакетов на целевые устройства, последующего копирования файлов на административный ресурс admin$ каждого из устройств и удаленной регистрации на них вспомогательных служб. Рассылка инсталляционных пакетов на целевые устройства выполняется с помощью функции Kaspersky SIEM Cloud, отвечающей за сетевое взаимодействие. При этом должны выполняться следующие условия:

- Доступ к целевым устройствам осуществляется со стороны точки распределения.
- В сети корректно работает разрешение имен для устройств.
- На целевых устройствах включены административные ресурсы общего доступа admin$.
- На целевых устройствах запущены следующие системные службы:
  - Сервер (LanmanServer).

    По умолчанию эта служба запущена.
  - DCOM Server Process Launcher (DcomLaunch).
  - RPC Endpoint Mapper (RpcEptMapper).
  - Вызов удаленной процедуры (Remote Procedure Call, RpcSs).
- TCP-порт 445 открыт на целевых устройствах для обеспечения удаленного доступа с помощью инструментария управления Windows (WMI).

  Также TCP-порт 445 проверяется, чтобы определить тип операционной системы целевого устройства перед выполнением удаленной установки (если UDP-порт 137 недоступен).

  > TCP 139, UDP 137 и UDP 138 используются старыми протоколами и больше не нужны для текущих приложений.

  На сетевом экране должны быть разрешены динамические исходящие порты доступа для соединения точек распространения с целевыми устройствами.
- В параметрах безопасности политики домена Active Directory разрешено обеспечивать работу NTLM-протокола при развертывании Агента администрирования.
- На целевых устройствах под управлением Microsoft Windows XP режим Simple File Sharing выключен.

- На целевых устройствах настроена модель совместного доступа и безопасности *Классическая – локальные пользователи выполняют аутентификацию самих себя*. Такая модель не может быть *Только гостевой – локальные пользователи выполняют аутентификацию как Гость*.

- Устройства являются членами домена, либо на устройствах заблаговременно созданы унифицированные учетные записи с административными правами.

Чтобы успешно развернуть Агент администрирования или другие приложения на устройстве, не подключенном к домену Active Directory с версией операционной системы Windows Server 2003 и выше, необходимо выключить удаленный UAC на этом устройстве. Удаленный UAC – это одна из причин, по которой учетные записи локальных администраторов не могут получить доступ к admin$, который требуется для принудительного развертывания Агента администрирования и других приложений. Выключение удаленного UAC не влияет на локальный UAC.

При установке на новые устройства, еще не размещенные в группах администрирования Kaspersky SIEM Cloud, в свойствах задачи удаленной установки можно задать группу администрирования, в которую устройства будут перемещаться по завершении установки на них Агента администрирования.

При создании групповой задачи необходимо помнить, что групповая задача действует на устройства всех вложенных подгрупп выбранной группы. Поэтому не следует дублировать задачи установки в подгруппах.

Упрощенным способом создания задач для принудительной установки приложений является автоматическая установка. Для этого в свойствах группы администрирования вам нужно открыть список инсталляционных пакетов и выбрать те пакеты, которые должны быть установлены на устройствах этой группы. В результате на всех устройствах этой группы и ее подгрупп будут автоматически установлены выбранные инсталляционные пакеты. Период, в течение которого будут установлены пакеты, зависит от пропускной способности сети и общего количества устройств в сети.

Устройства выполняющие роль точек распространения должны соответствовать требованиям для точек распространения. Вам нужно убедиться, что точки распространения присутствуют в каждой из изолированных подсетей, на которых размещены целевые устройства.

Объем свободного места в разделе с папкой %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit должен многократно превосходить суммарный объем дистрибутивов устанавливаемых приложений.

Мастер развертывания защиты

Для установки приложений "Лаборатории Касперского" можно воспользоваться мастером развертывания защиты. Мастер развертывания защиты позволяет проводить удаленную установку приложений как с использованием специально созданных инсталляционных пакетов, так и напрямую из дистрибутивов.

Мастер развертывания защиты выполнит следующие действия:

- Загружает инсталляционный пакет для установки приложения (если он не был создан раньше). Инсталляционный пакет расположен: **Управление программным обеспечением → Инсталляционные пакеты**. Вы можете использовать этот инсталляционный пакет для установки приложения в дальнейшем.

- Создает и запускает задачу удаленной установки для набора устройств или для группы администрирования. Созданная задача удаленной установки хранится в разделе **Задачи**. Вы можете запустить эту задачу в дальнейшем вручную. Тип задачи – **Удаленная установка приложения**.

Шаг 1. Запуск мастера развертывания защиты

Мастер развертывания защиты можно запустить вручную.

Чтобы запустить мастер развертывания защиты вручную,

В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Мастер развертывания защиты**.

Запустится мастер развертывания защиты. Для продолжения работы мастера нажмите на кнопку **Далее**.

Шаг 2. Выбор инсталляционного пакета

Выберите способ установки выбранного инсталляционного пакета:

- **Удаленная установка с помощью Kaspersky Security Center**
- **Удаленная установка с помощью Microsoft Azure API**

Далее выберите инсталляционный пакет приложения, которое требуется установить.

Если инсталляционный пакет требуемого приложения не содержится в списке, нажмите на кнопку **Добавить** и выберите приложение из списка.

Шаг 3. Выбор версии Агента администрирования

Если вы выбрали инсталляционный пакет приложения, отличный от Агента администрирования, необходимо также установить Агент администрирования для подключения приложения к Серверу администрирования Kaspersky Security Center.

Выберите последнюю версию Агента администрирования.

Шаг 4. Выбор устройств

Укажите список устройств, на которые требуется установить приложение:

- **Установить на управляемые устройства**

  Если выбран этот вариант, задача удаленной установки приложения будет создана для группы устройств.

- **Выбор устройств для установки**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

Шаг 5. Задание параметров задачи удаленной установки

На странице **Параметры задачи удаленной установки** настройте параметры удаленной установки приложения.

В блоке параметров **Принудительная загрузка инсталляционного пакета** выберите способ доставки на клиентские устройства файлов, необходимых для установки приложения:

- **С помощью Агента администрирования**

  Если этот параметр включен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

  Если этот параметр выключен, инсталляционные пакеты доставляются с помощью инструментов операционной системы клиентского устройства.

  Рекомендуется включить этот параметр, если задача назначена для устройств с установленными Агентами администрирования.

  По умолчанию параметр включен.

- **Средствами операционной системы с помощью точек распространения**

  Если этот параметр включен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения.

  Если параметр **С помощью Агента администрирования** включен, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

  По умолчанию параметр включен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

  Единственный способ установить приложение для Windows (включая Агент администрирования для Windows) на устройство, на котором не установлен Агент администрирования, – это использовать точку распространения с операционной системой Windows. Поэтому при установке приложения для Windows:

  - Выберите этот параметр.
  - Убедитесь, что для целевых клиентских устройств назначена точка распространения.
  - Убедитесь, что на точке распространения установлена операционная система Windows.

Настройте дополнительный параметр:

Не устанавливать приложение, если оно уже установлено

Если этот параметр включен, выбранное приложение не устанавливается заново, если оно уже установлено на клиентском устройстве.

Если этот параметр выключен, приложение будет установлено в любом случае.

По умолчанию параметр включен.

Пароль для удаления приложения "Лаборатории Касперского"

Поле **Пароль для удаления приложения "Лаборатории Касперского"** доступно, только если вы выбрали параметр **С помощью Агента администрирования** в группе параметров **Принудительно скачать инсталляционный пакет**.

Введите пароль в поле **Пароль для удаления приложения "Лаборатории Касперского"**, если вы переносите данные из одного приложения "Лаборатории Касперского" в другое и ваше текущее приложение защищено паролем. Обратите внимание, что во время переноса данных ваше текущее приложение "Лаборатории Касперского" будет удалено.

Для успешного завершения сценария переноса данных убедитесь, что выполнены следующие предварительные условия:

- Вы используете Агент администрирования Kaspersky Security Center для Windows версии 14.2 или выше.
- Вы устанавливаете приложение на устройства под управлением Windows.

Шаг 6. Управление перезагрузкой

Укажите действие, которое требуется выполнить, если необходимо перезагрузить операционную систему во время установки приложения:

- **Не перезагружать устройство**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

  - **Повторять запрос каждые (мин)**

    Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

    По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

    Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

  После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать приложения в заблокированных сеансах**

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

Шаг 7. Удаление несовместимых приложений перед установкой

Этот шаг присутствует, только если приложение, которое вы разворачиваете, несовместимо с другими приложениями.

Выберите этот параметр, если вы хотите, чтобы приложение Kaspersky SIEM Cloud автоматически удаляло несовместимые приложения с приложением, которое вы устанавливаете.

Отображается список несовместимых приложений.

Если этот параметр не выбран, приложение будет установлено только на устройствах, на которых нет несовместимых приложений.

Шаг 8. Перемещение устройств в папку Управляемые устройства

Укажите, следует ли перемещать устройства в группу администрирования после установки Агента администрирования.

- **Не перемещать устройства**

  Устройства остаются в тех группах, к которым они принадлежат. Устройства, не принадлежащие ни к одной из групп, остаются нераспределенными.

- **Перемещать нераспределенные устройства в группу**

  Устройства перемещаются в выбранную вами группу администрирования.

По умолчанию выбран вариант **Не перемещать устройства**. По соображениям безопасности вы можете предпочесть перемещение устройств вручную.

Шаг 9. Выбор учетных записей для доступа к устройствам

Если необходимо, добавьте учетные записи, которые будут использоваться для запуска задачи удаленной установки:

- **Учетная запись не требуется (Агент администрирования уже установлен)**

  Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор приложения. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

  Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

- **Учетная запись требуется (Агент администрирования не используется)**

  Выберите этот вариант, если Агент администрирования не установлен на устройствах, для которых вы назначаете задачу удаленной установки. В этом случае для установки приложения можно использовать локальную или доменную учетную запись пользователя, а при установке на клиентское устройство под управлением Linux — локальную или доменную учетную запись пользователя вместе с SSH-сертификатом.

  Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

  > Имя доменной учетной записи указывается в формате `domain\user name` или `user name@domain`.

  - **Локальная или доменная учетная запись**. Если выбран этот вариант, укажите учетную запись пользователя, от имени которой будет запускаться установщик приложения. Для этого нажмите на кнопку **Добавить**, выберите **Локальная или доменная учетная запись** и укажите имя и пароль локальной или доменной учетной записи пользователя.

  - **SSH сертификат**. Если вы хотите установить приложение на клиентское устройство под управлением Linux, вы можете указать SSH-сертификат и учетную запись пользователя. Для этого нажмите на кнопку **Добавить**, выберите **SSH сертификат** и заполните следующие поля:

    - В поле **Учетная запись** укажите имя локальной или доменной учетной записи пользователя.
    - В поле **Пользовательский сертификат** загрузите файл пользовательского сертификата.
    - В поле **Закрытый ключ** загрузите закрытый ключ пользовательского сертификата.
    - В поле **Пароль** укажите пароль для закрытого ключа пользовательского сертификата.

      > Пользовательский сертификат должен быть добавлен на клиентское устройство, на котором будет выполняться установка приложения. Для этого можно использовать утилиту ssh-copy-id.

      > Open Single Management Platform поддерживает формат закрытых ключей PEM. Формат OpenSSH не поддерживается.

Шаг 10. Запуск установки

Это последний шаг мастера. На этом шаге **Задача удаленной установки приложения** была успешно создана и настроена.

По умолчанию вариант **Запустить задачу после завершения работы мастера** не выбран. Если вы выберете этот параметр, **Задача удаленной установки приложения** начнется сразу после завершения работы мастера. Если вы не выберете этот параметр, **Задача удаленной установки приложения** не начнется. Вы можете запустить эту задачу в дальнейшем вручную.

Нажмите на кнопку **OK**, чтобы завершить последний шаг мастера развертывания защиты.

Сетевые параметры для взаимодействия с внешними сервисами

Open Single Management Platform использует следующие сетевые параметры для взаимодействия с внешними сервисами.

Сетевые параметры

Сетевые параметры	Адрес	Описание
Порт: 443 Протокол: HTTPS	activation-v2.kaspersky.com	Активация приложения.
Порт: 443 Протокол: HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	Обновление баз, модулей приложений и приложений "Лаборатории Касперского".
Порт: 443 Протокол: HTTPS	https://downloads.upd.kaspersky.com	• Обновление баз, модулей приложений и приложений "Лаборатории Касперского". • Проверка если серверы "Лаборатории Касперского" доступны. Open Single Management Platform проверяет доступность серверов "Лаборатории Касперского" перед загрузкой баз и модулей приложений "Лаборатории Касперского". Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы.

Сетевые параметры	Адрес	Описание
Порт: 80 Протокол: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Обновление баз, модулей приложений и приложений "Лаборатории Касперского".
Порт: 443 Протокол: HTTPS	ds.kaspersky.com dc1.ksn.kaspersky-labs.com dc1-file.ksn.kaspersky-labs.com dc1-pp.ksn.kaspersky-labs.com dc1-st.ksn.kaspersky-labs.com	Использование Kaspersky Security Network.
Порт: 443, 1443 Протокол: HTTPS	ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Использование Kaspersky Security Network.
Порт: 443 Протокол: HTTPS	click.kaspersky.com redirect.kaspersky.com	Переход по ссылкам из интерфейса.
Порт: 80 Протокол: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Инфраструктура открытых ключей (Public Key Infrastructure, PKI).
Порт: 443 Протокол: HTTPS	https://ipm-klca.kaspersky.com	Рекламные объявления.

Сетевые параметры	Адрес	Описание
Порт: 443 Протокол: HTTPS	https://tip.kaspersky.com	Реагирование на угрозы с помощью Kaspersky Threat Intelligence Portal (с использованием функциональности Kaspersky Security для бизнеса Профессиональный).
Порт: 443 Протокол: HTTPS	Полный список адресов см. в статье Структура адресов и доменов	Реагирование на угрозы с помощью Kaspersky Automated Security Awareness Platform (с использованием функциональности Kaspersky Security для бизнеса Профессиональный).

Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования

Перед установкой Агента администрирования на устройство под управлением Astra Linux в режиме замкнутой программной среды вам нужно выполнить две подготовительные процедуры: одну, которая описана в приведенных ниже инструкциях, и общие подготовительные шаги для любого устройства с операционной системой Linux.

Выполните команды, представленные в этой инструкции, под учетной записью root.

Чтобы подготовить устройство под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования:

1. Откройте файл `/etc/digsig/digsig_initramfs.conf` и укажите следующие параметры:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. В командной строке введите следующую команду, чтобы установить пакет совместимости:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Создайте директорию для ключа приложения:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Поместите ключ приложения /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg в директорию, созданную на предыдущем шаге:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   Если в комплект поставки Open Single Management Platform не входит ключ kaspersky_astra_pub_key.gpg, вы можете загрузить этот ключ по ссылке https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Обновите оперативную память дисков:

   ```
   update-initramfs -u -k all
   ```

   Перезагрузите систему.

Linux-устройство готово к установке Агента администрирования. Вы можете установить Агент администрирования удаленно, в интерактивном режиме или в тихом режиме.

Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux

Установка Агента администрирования состоит из двух шагов:

- Подготовка устройства с операционной системой Linux
- Удаленная установка Агента администрирования

Подготовка устройства с операционной системой Linux

Чтобы подготовить устройство с операционной системой Linux к удаленной установке Агента администрирования:

1. Убедитесь, что на устройстве, на которое вы хотите установить Агент администрирования Linux, работает один из поддерживаемых дистрибутивов Linux.
2. Загрузите инсталляционный пакет Агента администрирования с помощью интерфейса приложения или с веб-сайта "Лаборатории Касперского".

   Если требуется установить Kaspersky Industrial CyberSecurity for Linux Nodes на устройство под управлением операционной системы Linux с glibc 2.5, скачайте один из следующих инсталляционных пакетов с сайта "Лаборатории Касперского":

   - klnagent64_16.1.0-5840_amd64_glibc2.5.deb
   - klnagent64-16.1.0-5840.x86_64_glibc2.5.rpm
   - klnagent_16.1.0-5840_i386_glibc2.5.deb
   - klnagent-16.1.0-5840.i386_glibc2.5.rpm

   Эти инсталляционные пакеты доступны для следующих операционных систем с glibc 2.5:

   - CentOS 5.2 32-разрядная/64-разрядная.
   - CentOS 5.4 32-разрядная/64-разрядная.
   - CentOS 6.4 32-разрядная/64-разрядная.
   - CentOS 6.6 32-разрядная/64-разрядная.
   - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.4) 64-разрядная.

   Для получения инсталляционного пакета у вас должна быть лицензия Kaspersky Industrial CyberSecurity for Linux Nodes.

3. Убедитесь, что на целевом устройстве с операционной системой Linux установлено следующее программное обеспечение:

   - Sudo (для Ubuntu 10.04, версия Sudo 1.7.2p1 или выше).
   - Интерпретатор языка Perl версии 5.10 или выше.
   - Утилита ps.

4. Выполните проверку конфигурации устройства:

   a. Проверьте, что возможно подключение к устройству через SSH (например, приложение PuTTY).

      Если вы не можете подключиться к устройству, откройте файл `/etc/ssh/sshd_config` и убедитесь, что следующие параметры имеют значения:

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

      > Не изменяйте файл /etc/ssh/sshd_config, если вы можете без проблем подключиться к устройству; в противном случае вы можете столкнуться с ошибкой аутентификации SSH при выполнении задачи удаленной установки.

      Сохраните файл (при необходимости) и перезапустите службу SSH, используя команду `sudo service ssh restart`.

      Убедитесь, что порт TCP 22 открыт и доступен на нераспределенном устройстве под управлением ОС Linux. Для успешной установки Агента администрирования для Linux должен быть доступен TCP-порт 22.

   b. Отключите пароль запроса sudo для учетной записи пользователя, которая используется для подключения к устройству.

   c. Используйте команду sudo `visudo`, чтобы открыть конфигурационный файл sudoers.

      В открывшемся файле добавьте следующую строку в конец файла: `<user name> ALL = (ALL) NOPASSWD: ALL`. В этом случае `<user name>` является учетной записью пользователя, которая будет использоваться для подключения к устройству по протоколу SSH. Если вы используете операционную систему Astra Linux, в файл /etc/sudoers добавьте последней строку со следующим текстом: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   d. Сохраните и закройте файл sudoers.

   e. Повторно подключитесь к устройству через SSH и проверьте, что служба sudo не требует пароль, с помощью команды `sudo whoami`.

5. Откройте файл `/etc/systemd/logind.conf` и выполните одно из следующих действий:

   - Укажите значение 'no' для параметра KillUserProcesses: `KillUserProcesses=no`.
   - Для параметра KillExcludeUsers введите имя пользователя учетной записи, под которой будет выполняться удаленная установка, например, `KillExcludeUsers=root`.

Если целевое устройство работает под управлением Astra Linux, добавьте строку `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` в файл `/home/<user name>/.bashrc`, где `<user name>` – учетная запись пользователя, которая будет использоваться для подключения устройства с помощью SSH.

Чтобы применить измененный параметр, перезапустите устройство под управлением Linux или выполните команду:

```
sudo systemctl restart systemd-logind.service
```

6. Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat, чтобы настроить Агент администрирования.

7. Если вы хотите установить Агент администрирования на устройства с операционной системой Astra Linux, работающей в режиме замкнутой программной среды, выполните дополнительные действия для подготовки устройств Astra Linux.

8. Если вы хотите установить Агент администрирования на устройства с операционной системой РЕД ОС 7.3.4 и выше или МСВСфера 9.2 и выше, установите пакет libxcrypt-compat для корректной работы Агента администрирования.

Удаленная установка Агента администрирования

Чтобы установить Агент администрирования на устройство с операционной системой Linux:

1. Загрузите и создайте инсталляционный пакет:

   a. Перед установкой пакета на устройство убедитесь, что на нем установлены зависимости (приложения, библиотеки) для этого пакета.

   Вы можете самостоятельно посмотреть зависимости для каждого пакета, используя утилиты, специфичные для того дистрибутива Linux, на который будет устанавливаться пакет. С информацией об утилитах вы можете ознакомиться в документации к вашей операционной системе.

   b. Для создания пакета удаленной установки используйте файлы:

   - klnagent.kpd;
   - akinstall.sh;
   - deb или rpm пакет Агента администрирования.

2. Создайте задачу удаленной установки приложения с параметрами:

   - В окне **Параметры** мастера создания задачи установите флажок **Средствами операционной системы с помощью Сервера администрирования**. Снимите все остальные флажки.
   - На странице **Выбор учетной записи для запуска задачи** укажите параметры учетной записи, которая используется для подключения к устройству через SSH.

3. Запустите задачу удаленной установки приложения. Используйте параметр для команды `su`, чтобы сохранить среду: `-m, -p, --preserve-environment`.

Установка приложений с помощью задачи удаленной установки

Kaspersky SIEM Cloud позволяет удаленно устанавливать приложения на устройства с помощью задач удаленной установки. Эти задачи создаются и назначаются устройствам с помощью специального мастера. Чтобы быстрее и проще назначить задачу устройствам (до 1000 устройств), вы можете указывать в окне мастера устройства удобным для вас способом:

- **Выбрать устройства, обнаруженные в сети Сервером администрирования**. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- **Задать адреса устройств вручную или импортировать из списка**. В этом случае вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым вы хотите назначить задачу.
- **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать выборку, созданную по умолчанию, или вашу собственную выборку.
- **Назначить задачу группе администрирования**. В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

Для того чтобы избежать проблем, которые могут возникнуть при установке приложения на клиентское устройство без установленного Агента администрирования, необходимо действовать, как описано в разделе принудительного развертывания с помощью задачи удаленной установки Open Single Management Platform.

Удаленная установка приложений

Этот раздел содержит информацию о том, как удаленно установить приложение на устройства в группе администрирования, устройства с определенными адресами или на выборку устройств.

Чтобы установить приложение на выбранные устройства:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В поле **Тип задачи** выберите **Удаленная установка приложения**.
4. Выберите один из следующих вариантов:

   - **Назначить задачу группе администрирования**

     Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

     Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, так как групповые задачи подчиняются параметрам групп безопасности, к которым они относятся.

- **Задать адреса устройств вручную или импортировать из списка**

  Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

  Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

- **Назначить задачу выборке устройств**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

Задача Удаленная установка приложения создана для указанных устройств. Если вы выбрали параметр **Назначить задачу группе администрирования**, задача является групповой.

5. На шаге **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

   Доступные параметры зависят от параметра, выбранного на предыдущем шаге.

6. На шаге **Инсталляционные пакеты** укажите следующие параметры:

   - Выберите, как вы хотите установить выбранное приложение:

     - **Удаленная установка с помощью Kaspersky Security Center**

     - **Удаленная установка с помощью Microsoft Azure API**

       Дополнительные сведения об установке приложений на виртуальные машины Microsoft Azure см. в разделе Удаленная установка приложений на виртуальные машины Azure.

   - В поле **Выбор инсталляционного пакета** выберите инсталляционный пакет приложения, которое требуется установить.

   - В блоке параметров **Принудительно скачать инсталляционный пакет** выберите способ доставки на клиентские устройства файлов, необходимых для установки приложения:

     - **С помощью Агента администрирования**

       Если этот параметр включен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

       Если этот параметр выключен, инсталляционные пакеты доставляются с помощью инструментов операционной системы клиентского устройства.

       Рекомендуется включить этот параметр, если задача назначена для устройств с установленными Агентами администрирования.

       По умолчанию параметр включен.

- **Средствами операционной системы с помощью точек распространения**

  Если этот параметр включен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения.

  Если параметр **С помощью Агента администрирования** включен, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

  По умолчанию параметр включен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

  Единственный способ установить приложение для Windows (включая Агент администрирования для Windows) на устройство, на котором не установлен Агент администрирования, – это использовать точку распространения с операционной системой Windows. Поэтому при установке приложения для Windows:

  - Выберите этот параметр.
  - Убедитесь, что для целевых клиентских устройств назначена точка распространения.
  - Убедитесь, что на точке распространения установлена операционная система Windows.

- В поле **Максимальное количество одновременных загрузок** укажите максимально допустимое количество клиентских устройств, на которые Сервер администрирования может одновременно передавать файлы.

- В поле **Максимальное количество попыток установок** укажите максимально допустимое количество запусков приложения установки.

  Если количество попыток, указанное в параметрах задачи, превышено, Kaspersky SIEM Cloud больше не запускает приложение установки на устройстве. Чтобы перезапустить задачу *Удаленная установка приложения*, увеличьте значение параметра **Максимальное количество попыток установок** и перезапустите задачу. Также вы можете создать другую задачу *Удаленная установка приложения*.

- Если вы переносите данные из одного приложения "Лаборатории Касперского" в другую, и ваше текущее приложение защищено паролем, введите пароль в поле **Пароль для удаления приложения "Лаборатории Касперского"**. Обратите внимание, что во время переноса данных ваше текущее приложение "Лаборатории Касперского" будет удалено.

  Поле **Пароль для удаления приложения "Лаборатории Касперского"** доступно, только если вы выбрали параметр **С помощью Агента администрирования** в группе параметров **Принудительно скачать инсталляционный пакет**.

  Вы можете использовать пароль деинсталляции только для сценария переноса данных Kaspersky Security для Windows Server в Kaspersky Endpoint Security for Windows при установке Kaspersky Endpoint Security for Windows с помощью задачи Удаленная установка приложений. Использование пароля деинсталляции при установке других приложений может привести к ошибкам установки.

Для успешного завершения сценария переноса данных убедитесь, что выполнены следующие предварительные условия:

- Вы используете Агент администрирования Kaspersky Security Center версии 14.2 для Windows или выше.
- Вы устанавливаете приложение на устройства под управлением Windows.

- Настройте дополнительные параметры:
  - **Не устанавливать приложение, если оно уже установлено**

    Если этот параметр включен, выбранное приложение не устанавливается заново, если оно уже установлено на клиентском устройстве.

    Если этот параметр выключен, приложение будет установлено в любом случае.

    По умолчанию параметр включен.

  - **Предварительно проверять тип операционной системы перед загрузкой**

    Перед передачей файлов на клиентские устройства Open Single Management Platform проверяет, применимы ли параметры утилиты установки к операционной системе клиентского устройства. Если параметры не применимы, Open Single Management Platform не передает файлы и не пытается установить приложение. Например, чтобы установить некоторые приложения на устройства группы администрирования, в которую входят устройства с различными операционными системами, вы можете назначить задачу установки группе администрирования, а затем включить этот параметр, чтобы пропускать устройства с операционной системой, отличной от требуемой.

    При удаленной установке Агента администрирования на нераспределенные устройства Open Single Management Platform или точка распространения автоматически определяет тип операционной системы устройства независимо от параметра **Предварительно проверять тип операционной системы перед загрузкой**.

  - **Предлагать пользователю закрыть работающие приложения**

    Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

    Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

    Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

    По умолчанию параметр выключен.

- Выберите, на какие устройства вы хотите установить приложение:
  - **Устанавливать на все устройства**

    Приложение устанавливается даже на устройства, управляемые другими Серверами администрирования.

    По умолчанию этот вариант выбран. Не нужно изменять этот параметр, если в вашей сети есть только один Сервер администрирования.

- **Устанавливать на устройства, управляемые только этим Сервером администрирования**

  Приложение устанавливается только на устройства, которые управляются данным Сервером администрирования. Выберите этот параметр, если в вашей сети установлено больше одного Сервера администрирования и вы хотите избежать конфликтов между ними.

- Укажите, следует ли перемещать устройства в группу администрирования после установки:

  - **Не перемещать устройства**

    Устройства остаются в тех группах, к которым они принадлежат. Устройства, не принадлежащие ни к одной из групп, остаются нераспределенными.

  - **Переместить нераспределенные устройства в выбранную группу (можно выбрать только одну группу)**

    Устройства перемещаются в выбранную вами группу администрирования.

  По умолчанию выбран вариант **Не перемещать устройства**. По соображениям безопасности вы можете предпочесть перемещение устройств вручную.

7. На этом шаге мастера укажите, требуется ли перезагрузка устройства при установке приложений:

- **Не перезагружать устройство**

  Если выбран этот вариант, устройство не будет перезагружаться после установки приложения безопасности.

- **Перезагрузить устройство**

  Если выбран этот вариант, устройство будет перезагружено после установки приложения безопасности.

- **Запрашивать у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

  - **Повторять запрос каждые (мин)**

    Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

    По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

    Если параметр выключен, предложение перезагрузки отображается только один раз.

  - **Принудительно перезагрузить через (мин)**

    После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

    По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать приложения в заблокированных сеансах**

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

8. При необходимости на шаге **Выбор учетных записей для доступа к устройствам** добавьте учетные записи, которые будут использоваться для запуска задачи *Удаленная установка приложения*.

   - **Учетная запись не требуется (Агент администрирования уже установлен)**

     Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор приложения. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

     Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

   - **Учетная запись требуется (Агент администрирования не используется)**

     Выберите этот вариант, если Агент администрирования не установлен на устройствах, для которых вы назначаете задачу удаленной установки. В этом случае для установки приложения можно использовать локальную или доменную учетную запись пользователя, а при установке на клиентское устройство под управлением Linux — локальную или доменную учетную запись пользователя вместе с SSH-сертификатом.

     Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

     > Имя доменной учетной записи указывается в формате `domain\user name` или `user name@domain`.

     - **Локальная или доменная учетная запись**. Если выбран этот вариант, укажите учетную запись пользователя, от имени которой будет запускаться установщик приложения. Для этого нажмите на кнопку **Добавить**, выберите **Локальная или доменная учетная запись** и укажите имя и пароль локальной или доменной учетной записи пользователя.

     - **SSH сертификат**. Если вы хотите установить приложение на клиентское устройство под управлением Linux, вы можете указать SSH-сертификат и учетную запись пользователя. Для этого нажмите на кнопку **Добавить**, выберите **SSH сертификат** и заполните следующие поля:

       - В поле **Учетная запись** укажите имя локальной или доменной учетной записи пользователя.
       - В поле **Пользовательский сертификат** загрузите файл пользовательского сертификата.
       - В поле **Закрытый ключ** загрузите закрытый ключ пользовательского сертификата.
       - В поле **Пароль** укажите пароль для закрытого ключа пользовательского сертификата.

Пользовательский сертификат должен быть добавлен на клиентское устройство, на котором будет выполняться установка приложения. Для этого можно использовать утилиту ssh-copy-id.

Open Single Management Platform поддерживает формат закрытых ключей PEM. Формат OpenSSH не поддерживается.

9. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

   Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

10. В списке задач выберите созданную задачу и нажмите на кнопку **Запустить**.

    Или дождитесь запуска задачи в соответствии с расписанием, указанным в параметрах задачи.

После выполнения задачи удаленной установки, выбранное приложение устанавливается на указанный набор устройств.

Установка приложений на подчиненные Серверы администрирования

Если у вас версия Сервера администрирования 15.4 или выше, вы можете устанавливать приложения на подчиненный Сервер администрирования только в том случае, если его версия 15.4 или выше.

Чтобы установить приложение на подчиненные Серверы администрирования:

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.

2. Убедитесь в том, что соответствующий устанавливаемому приложению инсталляционный пакет находится на каждом из выбранных подчиненных Серверов администрирования. Если вы не можете найти инсталляционный пакет ни на одном из подчиненных Серверов, распространите его. Для этого создайте задачу с типом задачи **Распространение инсталляционного пакета**.

3. Создайте задачу удаленной установки приложения на подчиненных Серверах администрирования. Выберите тип задачи **Удаленная установка приложения на подчиненный Сервер администрирования**.

   В результате работы мастера создания задачи будет создана задача удаленной установки выбранного приложения на выбранные подчиненные Серверы администрирования.

4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

После выполнения задачи удаленной установки выбранное приложение устанавливается на подчиненные Серверы администрирования.

Запуск и остановка приложений "Лаборатории Касперского"

Вы можете использовать задачу *Запуск и остановка приложений* для запуска и остановки приложений "Лаборатории Касперского" на управляемых устройствах.

Чтобы создать задачу запуска или остановки приложения:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В раскрывающемся списке **Приложение** выберите приложение, для которого вы хотите создать задачу.
4. В списке **Тип задачи** выберите задачу **Запуск и остановка приложения**.
5. В поле **Название задачи** укажите название новой задачи.

   Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
6. Выберите устройства, которым будет назначена задача.
7. В окне **Приложения** выполните следующее:
   - Установите флажки рядом с названиями приложений, для которых вы хотите создать задачу.
   - Выберите параметр **Запустить приложение** или **Остановить приложение**.
8. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на шаге **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
9. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.
10. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
11. В окне свойств задачи укажите общие параметры задачи в соответствии с вашими требованиями и сохраните параметры.

Задача создана и настроена.

Чтобы запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

Обнаружение сетевых устройств и создание групп администрирования

В этом разделе описаны поиск устройств и опрос сети, а также создание групп администрирования для этих устройств.

Open Single Management Platform позволяет искать устройства на основании заданных критериев. Вы можете сохранить результаты поиска в текстовый файл.

Функция поиска позволяет находить следующие устройства:

- управляемые устройства в группах администрирования Сервера администрирования Open Single Management Platform и его подчиненных Серверов;
- нераспределенные устройства под управлением Сервера администрирования Open Single Management Platform и его подчиненных Серверов.

Сценарий: обнаружение сетевых устройств

Вам нужно выполнить поиск устройств перед первоначальным развертыванием приложений безопасности средствами приложения Kaspersky Security Center Cloud Console. При обнаружении сетевых устройств можно получить о них информацию и управлять ими с помощью политик. Регулярные опросы сети необходимы для проверки появления новых устройств и наличия обнаруженных ранее устройств в сети.

После завершения сценария обнаружение устройств настроено и будет выполняться в соответствии с указанным расписанием.

В Kaspersky SIEM Cloud вы можете добавить не более 33 000 устройств.

Предварительные требования

В Kaspersky Security Center Cloud Console обнаружение устройств выполняется точками распространения. Прежде чем начать, сделайте следующее:

- Решите, какие устройства будут выполнять роль точки распространения с учетом структуры вашей сети и ее изолированных сегментов.
- Выполните развертывание точек распространения на выбранные устройства по инструкции: Сценарий: первоначальное развертывание приложений "Лаборатории Касперского".

Этапы

Сценарий состоит из следующих этапов:

1. **Выбор типа обнаружения**

   Определите, какой тип обнаружения устройств вы хотите регулярно использовать для каждого сегмента сети.

2. **Настройка опросов**

   В свойствах каждой точки распространения включите и настройте выбранные типы сетевого опроса: опрос сети Windows, опрос контроллеров домена или опрос IP-диапазонов. Убедитесь, что расписание опроса соответствует нуждам вашей организации.

   Если сетевые устройства включены в домен, рекомендуется использовать опрос контроллеров домена.

3. **Задание правил для добавления обнаруженных устройств в группы администрирования (если требуется)**

   Если в сети появились новые устройства, они будут обнаружены при опросах сети. Такие устройства автоматически попадают в группу **Нераспределенные устройства**. При необходимости можно настроить правила автоматического перемещения этих устройств в группу **Управляемые устройства** и во вложенные группы администрирования. Устройства без сетевой активности удаляются через 60 дней в соответствии с правилами хранения по умолчанию.

   Если вы пропустили шаг, на котором задаются правила, все новые обнаруженные устройства будут помещены в группу **Нераспределенные устройства**. Вы можете переместить эти устройства в группу **Управляемые устройства** вручную. Если вы вручную переместили устройства в группу **Управляемые устройства**, вы можете проанализировать информацию о каждом из устройств и решить, требуется ли переместить его в группу администрирования и в какую.

Когда опрос завершен, вы можете просмотреть список новых обнаруженных устройств, распределенных в соответствии с заданными правилами. Если правила не заданы, устройства остаются в группе **Нераспределенные устройства**.

Опрос сети

Информацию о структуре сети и входящих в ее состав устройствах Сервер администрирования Open Single Management Platform получает в ходе регулярных опросов сети Windows, IP-диапазонов и контроллеров домена Microsoft Active Directory и контроллеров домена Samba. Для контроллеров домена Samba, в качестве контроллеров домена Active Directory используется Samba 4. Опрос сети можно запустить либо вручную, либо автоматически по расписанию.

В Kaspersky SIEM Cloud вы можете добавить не более 33 000 устройств и не более 17 000 учетных записей пользователей.

В зависимости от результатов опроса Open Single Management Platform обновляет список нераспределенных устройств. Можно также настроить правила автоматического перемещения новых обнаруженных устройств в определенные группы администрирования.

Open Single Management Platform использует следующие способы опроса сети:

- *Опрос IP-диапазонов*. Open Single Management Platform опрашивает сформированные IP-диапазоны с помощью ICMP-пакетов и получает полную информацию об устройствах, входящих в IP-диапазоны.

- *Опрос сети Windows*. Существуют два вида опроса сети Windows: быстрый опрос и полный опрос. При быстром опросе Open Single Management Platform получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. Во время полного опроса с каждого клиентского устройства запрашивается следующая информация: имя операционной системы, IP-адрес, DNS-имя, NetBIOS-имя.

- *Опрос контроллеров домена*. В базу данных Open Single Management Platform записывается информация о структуре групп Active Directory, а также информация о DNS-именах устройств, входящих в группы Active Directory.

Результаты опроса отображаются в разделе **Обнаружение устройств и развертывание → Обнаружение устройств** отдельно для *опроса Windows-сети* и *опроса контроллеров домена*.

Результаты опроса для *опроса IP-диапазонов* отображаются в разделе **Управление активами → Нераспределенные устройства**.

Одно и то же устройство может входить в результаты нескольких способов опроса. Если устройство обнаружено в домене HQ и его IP-адрес 192.168.0.1, устройство будет отображаться в разделе **Windows-домены** и в разделе **Нераспределенные устройства**. Можно настроить параметры опроса сети для каждого способа опроса. Например, может потребоваться изменить расписание опроса или указать, нужно опрашивать весь лес Active Directory или только определенный домен.

Опрос сети Windows

Об опросе сети Windows

Сервер администрирования Kaspersky SIEM Cloud не поддерживает опрос сети Windows. Используйте точки распространения с операционной системой Windows для опроса сетей Windows.

При быстром опросе точки распространения получают только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. Во время полного опроса с каждого клиентского устройства запрашивается следующая информация:

- имя операционной системы;

- IP-адрес;

- DNS-имя;

- NetBIOS-имя.

Как во время быстрого опроса, так и во время полного опроса необходимо:

- наличие открытых портов UDP 137/138, TCP 139, UDP 445, TCP 445;

- SMB-протокол включен;

- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на Сервере администрирования;
- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на клиентском устройстве:
  - наличие хотя бы одного устройства, если количество сетевых устройств не превышает 32;
  - наличие как минимум одного устройства на каждые 32 сетевых устройства.

Полный опрос сети может быть запущен, только если быстрый опрос был запущен как минимум один раз.

Просмотр и изменение параметров опроса сети Windows

Чтобы изменить параметры опроса сети Windows:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.
3. Нажмите на имя точки распространения, которую вы хотите использовать для опроса сети.

   Откроется окно свойств точки распространения.

4. Выберите раздел **Опрос Windows-доменов**.
5. Включите или выключите опрос Windows сети, используя переключатель **Разрешить опрос сети**.
6. Настройте расписание быстрого опроса и полного опроса.

   Варианты расписания опроса:

   - **Каждые N дней**

     Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

     По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

   - **Каждые N минут**

     Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

   - **По дням недели**

     Опрос выполняется регулярно, в указанные дни недели, в указанное время.

   - **Ежемесячно в выбранный день**

     Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

   - **Запускать пропущенные задачи**

     Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

По умолчанию параметр выключен.

7. Сохраните параметры опроса сети Windows.

Параметры сохранены и применены ко всем Windows-доменам и рабочим группам.

Опрос контроллеров домена

Kaspersky Security Center Cloud Console поддерживает опрос контроллеров домена только с помощью точек распространения. Вы можете настроить опрос следующих типов контроллеров домена:

- Microsoft Active Directory.
- Samba.
- FreeIPA.
- ALD Pro.

Kaspersky Security Center Cloud Console опрашивать контроллер домена Samba только с помощью точки распространения с операционной системой Linux. Для контроллеров домена Samba, в качестве контроллеров домена Active Directory используется Samba 4.

При опросе контроллеров домена точка распространения получает информацию о структуре домена, учетных записях пользователей, группах безопасности и о DNS-именах устройств, входящих в домен. Опрос контроллеров домена выполняется по заданному вами расписанию.

В Kaspersky SIEM Cloud вы можете добавить не более 33 000 устройств и не более 17 000 учетных записей пользователей.

Предварительные требования

Перед опросом контроллеров домена убедитесь, что включены следующие протоколы:

- Simple Authentication and Security Layer (SASL).
- Lightweight Directory Access Protocol (LDAP).

Убедитесь, что на устройстве контроллеров домена доступны следующие порты:

- 389 для SASL.
- 636 для TLS.

Опрос контроллеров домена с помощью точки распространения

Также можно опрашивать контроллеры домена с помощью точки распространения. Управляемое устройство с операционной системой Windows или Linux может выступать в роли точки распространения.

Для точки распространения с операционной системой Linux поддерживается опрос для всех типов контроллеров домена.
Для точки распространения с операционной системой Windows поддерживается только опрос контроллеров домена Microsoft Active Directory.
Опрос с помощью точки распространения с операционной системой Mac не поддерживается.

Чтобы настроить опрос контроллеров домена с помощью точки распространения:

1. Откройте свойства точки распространения.
2. Выберите раздел **Опрос контроллеров домена**.
3. В поле **Опрос** установите переключатель в положение **Включено**.
4. Если вы используете точку распространения с операционной системой Linux, выберите тип контроллера домена для опроса.
5. Выберите контроллеры домена, которые вы хотите опросить.

   Если вы используете точку распространения с операционной системой Linux, в разделе **Опросить указанные домены** нажмите на кнопку **Добавить**, а затем укажите адрес и учетные данные пользователя контроллеров домена.

   Если вы используете точку распространения с операционной системой Windows, можно выбрать один из следующих вариантов:

   - **Опросить текущий домен**
   - **Опросить весь лес доменов**
   - **Опросить указанные домены**
6. Нажмите на кнопку **Настроить расписание опроса**, чтобы указать параметры расписания опроса при необходимости.

   Опрос запускается в соответствие с расписанием. Запуск опроса вручную недоступен.

После завершения опроса в разделе **Контроллеры доменов** отобразится структура домена.

Если вы настроили и включили правила перемещения устройств, новые обнаруженные устройства будут автоматически перемещаться в группу **Управляемые устройства**. Если правила перемещения устройств не включены, новые обнаруженные устройства будут автоматически перемещаться в группу **Нераспределенные устройства**.

Обнаруженные учетные записи пользователей могут быть использованы для доменной аутентификации в OSMP Console.

Просмотр результатов опроса контроллеров домена

Чтобы просмотреть результаты опроса контроллеров домена:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Контроллеры доменов**.

   Отобразится список обнаруженных организационных подразделений.

2. Выберите организационное подразделение и нажмите на кнопку **Устройства**.

   Отобразится список устройств организационного подразделения.

Вы можете выполнить поиск устройств в списке и фильтровать результаты.

Опрос IP-диапазонов

Open Single Management Platform пытается выполнить обратное преобразование имен: для каждого IP-адреса из указанного диапазона выполнить преобразование в DNS-имя с помощью стандартных DNS-запросов. Если данная операция завершается успешно, сервер отправляет запрос `ICMP ECHO REQUEST` (аналог команды ping) на полученное имя. Если устройство отвечает, информация об этом устройстве добавляется в базу данных Open Single Management Platform. Обратное преобразование имен необходимо для исключения сетевых устройств, которые могут иметь IP-адреса, но не являются компьютерами, таких как сетевые принтеры или роутеры.

Этот способ опроса основывается на правильно настроенной локальной службе DNS. Для его использования должна быть настроена зона обратного просмотра DNS. Если эта зона не настроена, опрос IP-подсети не даст результатов. В сетях, в которых используется Active Directory, такая зона поддерживается автоматически. Но в таких сетях опрос IP-подсети не предоставляет дополнительной информации, помимо информации из опроса Active Directory. Кроме того, администраторы малых сетей часто не выполняют настройку зон обратного просмотра DNS, поскольку это не является необходимым для работы многих сетевых служб. Из-за этих причин опрос IP-подсети по умолчанию отключен.

Исходно Open Single Management Platform получает IP-диапазоны для опроса из сетевых параметров устройства, выполняющего роль точки распространения, которое используется для опроса сети. Если адрес устройства 192.168.0.1, а маска подсети – 255.255.255.0, Open Single Management Platform автоматически включит сеть 192.168.0.0/24 в список адресов для опроса. Open Single Management Platform выполнит опрос всех адресов от 192.168.0.1 до 192.168.0.254.

Не рекомендуется использовать опрос IP-диапазонов, если вы используете опрос сети Windows и/или опрос Active Directory.

Просмотр и изменение параметров опроса IP-диапазонов

Чтобы просмотреть и изменить параметры опроса IP-диапазонов:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Нажмите на имя точки распространения, которую вы хотите использовать для опроса сети.

   Откроется окно свойств точки распространения.

4. Выберите раздел **Опрос IP-диапазонов**.

5. Включите или выключите опрос IP-диапазонов, используя переключатель **Разрешить опрос диапазона**.

6. Настройте расписание опроса. По умолчанию опрос IP-диапазонов запускается каждые 420 минут (семь часов).

7. Если необходимо, добавьте или измените IP-диапазоны для опроса.

   При указании интервала опроса убедитесь, что его значение не превышает значения параметра время действия IP-адреса. Если IP-адрес не подтвержден при опросе в течение времени действия IP-адреса, он автоматически удаляется из результатов опроса. По умолчанию срок существования запросов составляет 24 часа, поскольку динамические IP-адреса, назначенные по протоколу DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации сетевого узла), меняются каждые 24 часа.

8. Нажмите на кнопку **OK**.

Параметры будут сохранены и применены ко всем IP-диапазонам.

Настройка контроллеров домена Samba

Kaspersky Security Center Cloud Console поддерживает контроллеры домена Linux, работающие только на Samba 4.

Контроллер домена Samba поддерживает те же расширения схемы, что и контроллер домена Microsoft Active Directory. Вы можете включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory, используя расширение схемы Samba 4. Это необязательное действие.

Рекомендуется включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory. Это обеспечит корректное взаимодействие Kaspersky Security Center Cloud Console и контроллера домена Samba.

Чтобы включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory:

1. Выполните команду, чтобы использовать расширение схемы RFC2307:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Включите обновление схемы на контроллере домена Samba. Для этого добавьте следующую строку в файл /etc/samba/smb.conf:

   ```
   dsdb:schema update allowed = true
   ```

   Если обновление схемы завершается с ошибкой, необходимо выполнить полное восстановление контроллера домена, который выполняет роль схемы master.

Для всех устройств с операционной системой Linux в контроллере домена Samba в файле `/etc/samba/smb.conf` нужно указать `netbios name` и параметры `workgroup`. Иначе результаты опроса могут содержать дублирующиеся устройства.

Добавление и изменение IP-диапазона

Исходно Open Single Management Platform получает IP-диапазоны для опроса из сетевых параметров устройства, выполняющего роль точки распространения, которое используется для опроса сети. Если адрес устройства 192.168.0.1, а маска подсети – 255.255.255.0, Open Single Management Platform автоматически включит сеть 192.168.0.0/24 в список адресов для опроса. Open Single Management Platform выполнит опрос всех адресов от 192.168.0.1 до 192.168.0.254. Вы можете изменять автоматически определенные IP-диапазоны или добавлять собственные IP-диапазоны.

Чтобы добавить новый IP-диапазон:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Нажмите на имя точки распространения, которую вы хотите использовать для опроса сети.

   Откроется окно свойств точки распространения.

4. Выберите раздел **Опрос IP-диапазонов**.

5. Чтобы добавить IP-диапазон, нажмите на кнопку **Добавить**.

6. В открывшемся окне настройте следующие параметры:

   - **Имя**

     Имя IP-диапазона. Вы можете указать IP-диапазон по имени, например, 192.168.0.0/24.

   - **IP-интервал или адрес и маска подсети**

     Задайте IP-диапазон, указав либо начальный и конечный IP-адреса, либо адрес подсети и маску подсети. Можно также выбрать один из существующих диапазонов IP-адресов, нажав на кнопку **Обзор**.

   - **Время действия IP-адреса (ч)**

     При задании этого параметра убедитесь, что он превышает значение интервала опроса, заданного в расписании опроса. Если IP-адрес не подтвержден при опросе в течение времени действия IP-адреса, он автоматически удаляется из результатов опроса. По умолчанию срок существования запросов составляет 24 часа, поскольку динамические IP-адреса, назначенные по протоколу DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации сетевого узла), меняются каждые 24 часа.

7. Нажмите на кнопку **OK**.

IP-диапазон добавлен в список IP-диапазонов.

После завершения опроса вы можете просмотреть список обнаруженных устройств, нажав на кнопку **Устройства**. По умолчанию срок действия результатов опроса составляет 24 часа, он равен времени действия IP-адреса.

Настройка точек распространения и шлюзов соединений

Структура групп администрирования в Kaspersky SIEM Cloud выполняет следующие функции:

- Задание области действия политик.

  Существует альтернативный способ применения нужных наборов параметров на устройствах с помощью *профилей политик*. В этом случае область применения политик задается с помощью тегов, местоположения устройств в подразделениях Active Directory, членства в группах безопасности Active Directory и прочего.

- Задание области действия групповых задач.

  Существует подход к заданию области действия групповых задач, не основанный на иерархии групп администрирования: использование задач для выборок устройств и наборов устройств.

- Задание прав доступа к устройствам и подчиненным Серверам администрирования.

- Назначение точек распространения.

При построении структуры групп администрирования следует учитывать топологию сети организации для оптимального назначения точек распространения. Оптимальное распределение точек распространения позволяет уменьшить сетевой трафик внутри сети организации.

В зависимости от организационной структуры организации и топологии сетей можно выделить следующие типовые конфигурации структуры групп администрирования:

- Один офис.

- Множество небольших изолированных офисов.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

Расчет количества и конфигурации точек распространения

Чем больше клиентских устройств содержит сеть, тем больше требуется точек распространения для распределения нагрузки. Используйте таблицы ниже, чтобы рассчитать количество точек распространения, необходимое для вашей сети.

Убедитесь, что устройства, которые вы хотите использовать в качестве точек распространения, соответствуют аппаратным требованиям, их не отключают регулярно и на них выключен "спящий режим". При отсутствии устройств с постоянной доступностью используйте расчет ниже для рабочих станций.

Использование устройств с постоянной доступностью в качестве точек распространения

Число специально выделенных точек распространения в сети, содержащей один сегмент сети, в зависимости от количества устройств в сети

Число клиентских устройств в сегменте сети	Количество точек распространения
Менее 300	0 (точки распространения не нужны)
Более 300	Приемлемо: (N/10 000 + 1), рекомендуется: (N/5000 + 2), где N количество устройств в сети

Число специально выделенных точек распространения в сети, содержащей несколько сегментов сети, в зависимости от количества устройств в сети

Число клиентских устройств в каждом сегменте сети	Количество точек распространения
Менее 10	0 (точки распространения не нужны)
10–100	1
Более 100	Приемлемо: (N/10 000 + 1), рекомендуется: (N/5000 + 2), где N количество устройств в сети

Использование клиентских устройств (рабочих станций) в качестве точек распространения

Если вы планируете использовать в качестве точек распространения обычное клиентское устройство (рабочую станцию), то рекомендуется назначать точку распространения, как показано в таблице ниже, чтобы избежать чрезмерной нагрузки на каналы связи и Сервер администрирования:

Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит один сегмент сети, в зависимости от количества сетевых устройств

Число клиентских устройств в сегменте сети	Количество точек распространения
Менее 300	0 (точки распространения не нужны)
Более 300	(N/300 +1), где N – число устройств в сети; не менее 3 точек распространения

Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит несколько сегментов сети, в зависимости от количества сетевых устройств

Число клиентских устройств в каждом сегменте сети	Количество точек распространения
Менее 10	0 (точки распространения не нужны)
10–30	1
31–300	2
Более 300	(N/300 +1), где N – число устройств в сети; не менее 3 точек распространения

В одной рабочей области не может быть более 100 точек распространения.

Если точка распространения бывает недоступна, рассмотрите возможность добавления резервных источников обновления баз, модулей приложений и приложений "Лаборатории Касперского" вручную или напрямую с серверов обновлений "Лаборатории Касперского".

Типовая конфигурация точек распространения: один офис

В типовой конфигурации "один офис" все устройства находятся в сети организации и "видят" друг друга. Сеть организации может состоять из нескольких выделенных частей (сетей или сегментов сети), связанных узкими каналами.

Возможны следующие способы построения структуры групп администрирования:

- Построение структуры групп администрирования с учетом топологии сети. Структура групп администрирования не обязательно должна точно отражать топологию сети. Достаточно того, чтобы выделенным частям сети соответствовали какие-либо группы администрирования. Каждой группе назначены свои точки распространения.

- Построение структуры групп администрирования, не отражающей топологию сети. В этом случае следует в каждом сегменте сети назначить необходимое количество точек распространения и назначить им всем область действия на корневую группу администрирования **Управляемые устройства**. Все точки распространения окажутся на одном уровне и будут иметь одинаковую область действия "все устройства сети организации". Каждый Агент администрирования будет подключаться к той точке распространения, маршрут к которой является самым коротким. Маршрут к точке распространения можно определить с помощью утилиты tracert.

Типовая конфигурация точек распространения: множество небольших удаленных офисов

Этой типовой конфигурации соответствует множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Каждый из удаленных офисов находится за NAT, то есть подключение из одного удаленного офиса в другой невозможно – офисы изолированы друг от друга.

Конфигурацию следует обязательно отразить в структуре групп администрирования: для каждого из удаленных офисов следует создать отдельную группу администрирования (группы **Офис 1**, **Офис 2** на рисунке ниже).

Удаленные офисы отражены в структуре групп администрирования

На каждую группу администрирования, соответствующую офису, нужно назначить не менее одной точки распространения. Точками распространения нужно назначать устройства удаленного офиса, которые соответствуют аппаратным требованиям. Устройства, размещенные, например, в группе **Офис 1**, будут обращаться к точкам распространения, назначенным на группу администрирования **Офис 1**.

Если некоторые пользователи физически перемещаются между офисами с ноутбуками, нужно в каждом удаленном офисе дополнительно к упомянутым выше точкам распространения выбрать два и или более устройств и назначить их точками распространения на группу администрирования верхнего уровня (группа **Корневая группа для офисов** на рисунке выше).

Ноутбук, находившийся в группе администрирования **Офис 1**, но физически перемещенный в офис, соответствующий группе **Офис 2**. После перемещения Агент администрирования на ноутбуке попытается обратиться к точкам распространения, назначенным на группу **Офис 1**, но эти точки распространения окажутся недоступны. Тогда Агент администрирования начнет обращаться к точкам распространения, назначенным на группу **Корневая группа для офисов**. Так как удаленные офисы изолированы друг от друга, то из всех точек распространения, назначенных на группу администрирования **Корневая группа для офисов**, успешными будут лишь обращения к точкам распространения, назначенным на группу **Офис 2**. То есть ноутбук, оставаясь в группе администрирования, соответствующей своему исходному офису, будет, тем не менее, использовать точку распространения того офиса, в котором в данный момент находится физически.

Назначение точек распространения вручную

Kaspersky SIEM Cloud позволяет вручную назначать устройства точками распространения. Рекомендуется рассчитать количество точек распространения и их конфигурацию, необходимые для вашей сети.

Точки распространения под управлением macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского".

Если устройства с операционной системой macOS находятся в области действия задачи *Загрузка обновлений в хранилища точек распространения*, задача завершится со статусом *Сбой*, даже если она успешно завершилась на всех устройствах с операционной системой Windows.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

Точка распространения должна иметь прямой сетевой доступ к Серверу администрирования или подключаться к нему через прокси-сервер. Шлюз соединений не обеспечивает работу других точек распространения. Если назначить устройство, выступающее в качестве шлюза соединения, точкой распространения, управление этим устройством будет потеряно до тех пор, пока вы не откроете сетевой доступ или не переустановите Агент администрирования.

Чтобы вручную назначить устройство точкой распространения:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.

3. Нажмите на кнопку **Назначить**.

4. Выберите устройство, которое вы хотите сделать точкой распространения.

   При выборе устройства учитывайте особенности работы точек распространения и требования к устройству, которое выполняет роль точки распространения.

5. Выберите группу администрирования или сетевое местоположение, которую вы хотите включить в область действия выбранной точки распространения.

6. Нажмите на кнопку **Добавить**.

   Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.

7. Выберите в списке добавленную точку распространения, чтобы открыть окно ее свойств.

8. В окне свойств настройте параметры точки распространения:

- В разделе **Общие** укажите параметры взаимодействия точки распространения с клиентскими устройствами:

  - **SSL-порт**

    Номер TLS-порта, по которому осуществляется защищенное подключение клиентских устройств к точке распространения с использованием протокола TLS.

    По умолчанию номер порта – 13000.

  - **Включено**

    Если параметр включен, для автоматического распространения инсталляционных пакетов на клиентские устройства в пределах группы будет использоваться многоадресная IP-рассылка.

    Многоадресная IP-рассылка уменьшает время, необходимое для установки приложений из инсталляционного пакета на группу клиентских устройств, но увеличивает время установки при установке приложения на одно клиентское устройство.

  - **Адрес IP-рассылки**

    IP-адрес, на который будет выполняться многоадресная рассылка. IP-адрес можно задать в диапазоне 224.0.0.0 – 239.255.255.255

    По умолчанию Kaspersky SIEM Cloud автоматически назначает уникальный IP-адрес многоадресной рассылки в заданном диапазоне.

  - **Номер порта IP-рассылки**

    Номер порта многоадресной рассылки.

    Номер порта по умолчанию – 15001. Если в качестве точки распространения указано устройство, на котором установлен Сервер администрирования, то для подключения с использованием TLS-протокола по умолчанию используется порт 13001.

  - **Адрес точки распространения для удаленных устройств**

    Сетевой адрес, через который удаленные устройства подключаются к точке распространения.

  - **Включено**

    Обновления распространяются на управляемые устройства из следующих источников:

    - Эта точка распространения, если этот параметр включен.
    - Другие точки распространения, Сервер администрирования или серверы обновлений "Лаборатории Касперского", если параметр выключен.

    Если вы используете точки распространения для распространения обновлений, вы можете сэкономить трафик, так как уменьшите количество загрузок. Также вы можете снизить нагрузку на Сервер администрирования и перераспределить нагрузку между точками распространения. Вы можете вычислить количество точек распространения в вашей сети для оптимизации трафика и нагрузки.

    Если вы выключите этот параметр, количество загрузок обновлений и нагрузка на Сервер администрирования могут увеличиться. По умолчанию параметр включен.

- **Включено**

  Инсталляционные пакеты распространяются на управляемые устройства из следующих источников:

  - Эта точка распространения, если этот параметр включен.
  - Другие точки распространения, Сервер администрирования или серверы обновлений "Лаборатории Касперского", если параметр выключен.

  Если вы используете точки распространения для распространения инсталляционных пакетов, вы можете сэкономить трафик, так как уменьшите количество загрузок. Также вы можете снизить нагрузку на Сервер администрирования и перераспределить нагрузку между точками распространения. Вы можете вычислить количество точек распространения в вашей сети для оптимизации трафика и нагрузки.

  Если вы выключите этот параметр, количество загрузок инсталляционных пакетов и нагрузка на Сервер администрирования могут увеличиться. По умолчанию параметр включен.

- **Включено**

  В Open Single Management Platform точка распространения может работать как push-сервер для устройств, которые управляются по мобильному протоколу, и для устройств под управлением Агента администрирования. Например, push-сервер должен быть включен, если вы хотите включить принудительную синхронизацию устройств с KasperskyOS с Сервером администрирования. Push-сервер имеет ту же область управляемых устройств, что и точка распространения, на которой включен push-сервер. Если у вас есть несколько точек распространения, назначенных для одной и той же группы администрирования, вы можете включить извещающий сервер на каждой них. В этом случае Сервер администрирования распределяет нагрузку между точками распространения.

- **Порт push-сервера**

  Номер порта push-сервера. Вы можете указать номер любого свободного порта.

- В разделе **Область действия** укажите область, на которую точка распространения распространяет обновления (группы администрирования и/или сетевое местоположение).

  Если вы хотите указать группу администрирования, нажмите на кнопку **Добавить группу**. В открывшейся правой панели выберите группу администрирования из раскрывающегося списка и нажмите на кнопку **Добавить**.

  Если вы хотите указать подсеть, нажмите на кнопку **Добавить подсеть**. В открывшейся правой панели нажмите на кнопку **Добавить** и укажите имя подсети.

  > Для устройств с операционной системой Windows отображается переключатель **Автоматически назначать точки распространения в рамках данного сетевого местоположения**. Определение сетевого местоположения недоступно для устройств под управлением других операционных систем.

- В разделе **Источник обновлений** можно выбрать источник обновлений для точки распространения.

- Если ваши точки распространения используют прокси-сервер для подключения к интернету, в разделе **Параметры подключения к интернету** вы можете указать следующие параметры:

  - **Использовать прокси-сервер**

    Если этот флажок установлен, для подключения точек распространения к серверу обновлений "Лаборатории Касперского" используется прокси-сервер в интернете. Вы можете настроить подключение к прокси-серверу в полях ввода.

По умолчанию флажок снят.

- **Адрес прокси-сервера**

  Адрес прокси-сервера.

- **Номер порта**

  Номер порта, по которому будет выполняться подключение.

- **Не использовать прокси-сервер для локальных адресов**

  Если параметр включен, то при подключении к устройствам в локальной сети не используется прокси-сервер.

  По умолчанию параметр выключен.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  По умолчанию флажок снят.

- **Имя пользователя**

  Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

- **Пароль**

  Пароль учетной записи, от имени которой будет запускаться задача.

- В разделе **Прокси-сервер KSN** вы можете настроить приложение так, чтобы точка распространения использовалась для пересылки KSN запросов от управляемых устройств.

  - **Включить прокси-сервер KSN на стороне точки распространения**

    Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

    Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского".

    По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены в окне свойств Сервера администрирования.

    Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

  - **Порт**

    Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

  - **Использовать UDP-порт**

    Чтобы управляемые устройства подключались к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и укажите номер UDP-порта. По умолчанию параметр включен.

- **UDP-порт**

  Номер UDP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

- **Использовать HTTPS**

  Если вам нужно, чтобы управляемые устройства подключались к прокси-серверу KSN через порт HTTPS, включите параметр **Использовать HTTPS** и укажите номер порта в поле **Через HTTPS-порт**. По умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.

- **HTTPS-порт**

  Номер HTTPS-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.

- В разделе **Шлюз соединения** вы можете настроить точку распространения для работы в роли шлюза для соединения между экземплярами Агента администрирования и Сервером администрирования, если прямое соединение не может быть установлено из-за организации вашей сети. Для этого включите переключатель **Шлюз соединения**.

  По умолчанию параметр выключен.

  При подключении мобильных устройств к Серверу администрирования через точку распространения, выполняющую роль шлюза соединения, вы можете включить следующие параметры:

  - **Открыть порт для мобильных устройств (SSL-аутентификация только Сервера администрирования)**

    Включите этот параметр, если требуется, чтобы шлюз соединения открывал порт для мобильных устройств, и укажите номер порта, который мобильные устройства будут использовать для подключения к точке распространения. По умолчанию установлен порт 13292. Мобильное устройство проверит сертификат Сервера администрирования. При установке соединения только Сервер администрирования выполняет аутентификацию.

  - **Открыть порт для мобильных устройств (двусторонняя SSL-аутентификация)**

    Включите этот параметр, если требуется, чтобы шлюз соединения открывал порт, который будет использоваться для двусторонней аутентификации Сервера администрирования и мобильных устройств. Мобильное устройство проверит сертификат Сервера администрирования, а Сервер администрирования проверит сертификат мобильного устройства. Задайте следующие параметры:

    - Номер порта, который мобильные устройства будут использовать для подключения к точке распространения. По умолчанию установлен порт 13293.

    - Имена DNS-доменов шлюза соединения, которые будут использоваться мобильными устройствами. Разделяйте имена доменов запятыми. Указанные имена доменов будут включены в сертификат точки распространения. Если имена доменов, используемые мобильными устройствами, не совпадают с общим именем в сертификате точки распространения, мобильные устройства не подключаются к точке распространения.

      Имя DNS-домена по умолчанию – это полное имя домена шлюза соединения.

  В обоих случаях сертификаты проверяются во время установки TLS-сеанса только на точке распространения. Сертификаты не пересылаются на проверку Сервером администрирования. После установки TLS-сеанса с мобильным устройством точка распространения использует сертификат Сервера администрирования для создания туннеля для синхронизации между мобильным устройством и Сервером администрирования. Если вы откроете порт для двусторонней SSL-аутентификации, единственный способ распространить сертификат мобильного устройства – это с помощью установочного пакета.

- Настройте опрос доменов Windows, контроллеров домена и IP-диапазонов точкой распространения:

  - **Опрос Windows-доменов**

    Вы можете включить обнаружение устройств для Windows-доменов, включив переключатель **Разрешить опрос сети** и нажав на кнопку **Настроить расписание полного опроса**, чтобы задать расписание для обнаружения.

    В открывшемся окне настройте следующие параметры:

    - **Запуск по расписанию**

      Вы можете выбрать один из следующих вариантов расписания:

      - **Каждые N дней**

        Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени. По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

      - **Каждые N минут**

        Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени. По умолчанию опрос запускается каждые пять минут, начиная с текущего системного времени.

      - **По дням недели**

        Опрос выполняется регулярно, в указанные дни недели, в указанное время. По умолчанию опрос запускается каждую пятницу в 18:00:00.

      - **Ежемесячно в выбранный день**

        Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время. По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

    - **Интервал запуска (сут)**

      Укажите значение N (для минут или дней).

      Поле отображается, если вы выбрали вариант расписания **Каждые N дней** или **Каждые N минут**.

    - **Начиная с момента**

      Укажите начало первого опроса.

      Поле отображается, если вы выбрали вариант расписания **Каждые N дней** или **Каждые N минут**.

    - **Запускать пропущенные задачи**

      Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

      По умолчанию этот параметр выключен. Это означает, что Сервер администрирования ждет следующего планового опроса.

      Если вы включите этот параметр, Сервер администрирования начинает опрос сразу после его включения.

    Раздел отображается только для точек распространения с операционной системой Windows.

- **Опрос контроллеров домена**

  Вы можете включить опрос Active Directory и задать расписание опроса.

  Если вы используете точку распространения с операционной системой Windows, можно выбрать один из следующих вариантов:

  - **Опросить текущий домен Active Directory**.
  - **Опросить лес доменов Active Directory**.
  - **Опросить указанные домены Active Directory**. Если вы выбрали этот вариант, добавьте один или несколько доменов Active Directory в список.

  Если вы используете точку распространения с операционной системой Linux с установленным Агентом администрирования версии 15, вы можете опрашивать только те домены Active Directory, для которых вы указываете адрес и учетные данные пользователя. Опрос текущего домена Active Directory и леса доменов Active Directory недоступен.

  Вы можете включить обнаружение устройств для контроллеров домена.

  Когда переключатель установлен в положение **Включено**, в поле **Опрос** вы можете выбрать контроллеры домена для опроса, а также указать для них расписание опроса.

  Если вы используете точку распространения с операционной системой Linux, в разделе **Опросить указанные домены** нажмите на кнопку **Добавить**, а затем укажите адрес и учетные данные пользователя контроллера домена. Также вы можете указать тип домена для опроса: Active Directory или Samba, FreeIPA, ALD Pro.

  Если вы используете точку распространения с операционной системой Windows, можно выбрать один из следующих вариантов:

  - **Опросить текущий домен**
  - **Опросить весь лес доменов**
  - **Опросить указанные домены**

- **Опрос IP-диапазонов**

  Вы можете включить обнаружение устройств для IPv4-диапазонов и IPv6-сетей.

  Если вы включили параметр **Разрешить опрос диапазона**, вы можете добавить диапазон опроса и задать расписание опроса. Вы можете добавить IP-диапазоны в список опрашиваемых диапазонов.

  Если включить параметр **Использовать Zeroconf для опроса IPv6-сетей**, точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией (далее также *Zeroconf*). В этом случае указанные IP-диапазоны игнорируются, так как точка распространения опрашивает всю сеть. Параметр **Использовать Zeroconf для опроса IPv6-сетей** доступен, если точка распространения работает под управлением Linux. Чтобы использовать опрос Zeroconf IPv6, вам нужно установить утилиту avahi-browse на точке распространения.

- В разделе **Дополнительно** укажите папку, которую точка распространения должна использовать для хранения распространяемых данных:

  - **Использовать папку по умолчанию**

    При выборе этого варианта для сохранения данных будет использоваться папка, в которую на точке распространения установлен Агент администрирования.

- **Использовать указанную папку**

  При выборе этого варианта в расположенном ниже поле можно указать путь к папке. Папка может размещаться как локально на точке распространения, так и удаленно, на любом из устройств, входящих в состав сети организации.

  Учетная запись, под которой на точке распространения запускается Агент администрирования, должна иметь доступ к указанной папке для чтения и записи.

- В разделе **Статистика** вы можете просмотреть статистику по загрузке антивирусных баз на устройство или статистику по установке пакетов на устройство.

9. Нажмите на кнопку **OK**.

В результате выбранные устройства будут выполнять роль точек распространения.

Изменение списка точек распространения для группы администрирования

Вы можете просмотреть список точек распространения, назначенных для определенной группы администрирования, и изменить список, добавив или удалив точки распространения.

Чтобы просмотреть и изменить список точек распространения для группы администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.

2. Выберите группу администрирования, для которой вы хотите просмотреть назначенные точки распространения, нажмите на кнопку **Показать иерархию** в верхней части страницы, а затем в открывшемся окне нажмите на имя нужной группы.

   В результате отображается пункт меню **Точки распространения**.

   Путь к выбранной группе отображается в верхней части страницы. Чтобы перейти к группе администрирования, в этом пути нажмите на ссылку с названием группы. По умолчанию последняя ссылка в пути неактивна.

3. В главном окне приложения перейдите в раздел **Управление активами** → **Точки распространения**.

4. Добавьте новые точки распространения для группы администрирования с помощью кнопки **Назначить** или удалите назначенные точки распространения с помощью кнопки **Отменить назначение**.

   После того как вы нажмете на кнопку **Отменить назначение** устройство будет удалено из группы администрирования и перестанет выполнять роль точки распространения.

В зависимости от изменений, точки распространения добавляются в список или существующие точки распространения удаляются из списка.

Если точка распространения используется в качестве шлюза соединения, перед ее удалением рекомендуем выполнить следующие действия:

1. Создайте новый шлюз соединения с той же областью действия.
2. Убедитесь, что управляемые устройства, использующие текущий шлюз соединения, могут установить сетевое соединение с новым шлюзом.
3. В политике Агента администрирования включите параметр **Использовать шлюз соединения точки распространения (при наличии) в параметрах подключения по умолчанию**. Рекомендуем выполнить это действие до удаления точки распространения.

Если шлюз соединения был удален без выполнения этих действий, восстановите его работу по прежнему адресу подключения. После этого все управляемые устройства, использовавшие этот шлюз, снова смогут работать.

Использование точки распространения в качестве извещающего сервера

В Open Single Management Platform точка распространения может работать как push-сервер для устройств, которые управляются по мобильному протоколу, и для устройств под управлением Агента администрирования. Например, push-сервер должен быть включен, если вы хотите включить принудительную синхронизацию устройств с KasperskyOS с Сервером администрирования. Push-сервер имеет ту же область управляемых устройств, что и точка распространения, на которой включен push-сервер. Если у вас есть несколько точек распространения, назначенных для одной и той же группы администрирования, вы можете включить извещающий сервер на каждой них. В этом случае Сервер администрирования распределяет нагрузку между точками распространения.

Вы можете использовать точки распространения в качестве push-серверов, чтобы установить постоянное соединение между управляемым устройством и Сервером администрирования. Постоянное соединение необходимо для некоторых операций, таких как запуск и остановка локальных задач, получение статистики для управляемого приложения или создание туннеля. Если вы используете точку распространения в качестве push-сервера, вам не нужно отправлять пакеты на UDP-порт Агента администрирования.

Чтобы использовать точку распространения в качестве push-сервера:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Точки распространения**.
3. Выберите точку распространения, которую вы хотите использовать в качестве push-сервера.
4. В списке свойств выбранной точки распространения перейдите в раздел **Общие** и включите параметр **Включено**.

   Поле ввода **Порт push-сервера** станет доступным.

5. В поле ввода **Порт push-сервера** укажите порт точки распространения, который клиентские устройства будут использовать для подключения. По умолчанию номер порта – 13295.

   В правилах сетевого экрана вам нужно разрешить исходящие сетевые соединения между управляемыми устройствами и портом push-сервера.

6. Нажмите **OK**, чтобы закрыть окно свойств точки распространения, а затем нажмите **Сохранить**, чтобы применить изменения.

   После включения параметра **Включено** параметр **Не разрывать соединение с Сервером администрирования** автоматически включится на точке распространения, которая используется в качестве push-сервера. Этот параметр позволяет установить предварительное соединение между Агентом администрирования и Сервером администрирования.

7. Откройте окно Параметры политики Агента администрирования.

8. Перейдите в раздел **Подключения** → **Сеть** и включите параметр **Использовать точку распространения для принудительного подключения к Серверу администрирования**. Установите замок для этого параметра.

9. В подразделе **Сеть** вы также можете отключить параметр **Использовать UDP-порт**. После настройки push-сервер перестанет отправлять пакеты через UDP-порт и будет поддерживать непрерывное соединение между управляемым устройством и Сервером администрирования.

10. Нажмите на кнопку **OK**, чтобы закрыть окно.

Точка распространения начинает выполнять роль push-сервера. Теперь он может отправлять push-уведомления на клиентские устройства.

Использование параметра "Не разрывать соединение с Сервером администрирования" для обеспечения постоянной связи между управляемым устройством и Сервером администрирования

Если вы не используете push-серверы, Kaspersky SIEM Cloud не обеспечивает постоянного соединения между управляемыми устройствами и Сервером администрирования. Агенты администрирования на управляемых устройствах периодически устанавливают соединение и синхронизируются с Сервером администрирования. Продолжительность периода такой синхронизации задается в политике Агента администрирования. Если требуется предварительная синхронизация, Сервер администрирования (или точка распространения, если она используется) отправляет подписанный сетевой пакет по IPv4-сети или IPv6-сети на UDP-порт Агента администрирования. Номер порта по умолчанию – 15000. Если подключение по UDP от Сервера администрирования к управляемому устройству невозможно, то синхронизация произойдет при очередном периодическом подключении Агента администрирования к Серверу в течение периода синхронизации.

Некоторые операции невозможно выполнить без предварительного соединения Агента администрирования с Сервером администрирования, например, запуск и остановка локальных задач, получение статистики по управляемому приложению или создание туннеля. Чтобы решить эту проблему, если вы не используете push-серверы, вы можете использовать параметр **Не разрывать соединение с Сервером администрирования**, который обеспечивает постоянное соединение между управляемым устройством и Сервером администрирования.

Чтобы проверить постоянное соединение управляемого устройства с Сервером администрирования:

1. Выполните одно из следующих действий:

   - Если управляемое устройство обращается к Серверу администрирования напрямую (то есть не через точку распространения), в главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства** и нажмите на имя устройства, с которым вы хотите обеспечить постоянную связь.

     Откроется окно свойств управляемого устройства.

- Если управляемое устройство обращается к Серверу администрирования через точку распространения, работающую в режиме шлюза, а не напрямую:

  a. Откройте окно свойств Сервера администрирования, нажав на имя Сервера администрирования в главном меню.

  Вы также можете перейти к свойствам нужного Сервера администрирования из панели навигации. Для этого в главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Settings**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**. В открывшейся панели наведите курсор мыши на название нужного Сервера администрирования и нажмите на значок параметров (⚙).

  b. На вкладке **Общие** выберите раздел **Точки распространения**.

  c. Выберите имя нужной точки распространения из списка точек распространения.

  Откроется окно свойств выбранной точки распространения.

2. В разделе **Общие** открывшегося окна свойств выберите параметр **Не разрывать соединение с Сервером администрирования**.

Постоянное соединение установлено между управляемым устройством и Сервером администрирования.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

Создание групп администрирования

Исходно иерархия групп администрирования содержит только группу администрирования **Управляемые устройства**. При создании иерархии групп администрирования в состав группы **Управляемые устройства** можно включать устройства и виртуальные машины и добавлять вложенные группы. Для каждой группы администрирования окно свойств содержит информацию о политиках, задачах и устройствах, относящихся к группе.

Чтобы создать группу администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.
2. Установите флажок напротив группы администрирования, для которой вы хотите создать подгруппу.
3. Нажмите на кнопку **Добавить**.
4. Введите имя новой группы администрирования.
5. Нажмите на кнопку **Добавить**.

Новая группа администрирования, с указанным именем, появится в иерархии групп администрирования.

Приложение позволяет создавать структуру групп администрирования на основе структуры Active Directory или структуры доменной сети. Также вы можете создавать структуру групп из текстового файла.

Чтобы создать структуру групп администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами → Иерархия групп**.
2. Нажмите на кнопку **Импортировать**.

В результате запускается мастер создания структуры групп администрирования. Следуйте далее указаниям мастера.

Создание правил перемещения устройств

Можно настроить правила перемещения устройств, в соответствии с которыми устройства будут распределены по группам администрирования.

Чтобы создать правило перемещения устройств:

1. В главном окне приложения перейдите в раздел **Управление активами → Правила перемещения**.
2. Нажмите на кнопку **Добавить**. Откроется окно **Новое правило**.
3. На вкладке **Общие** укажите следующую информацию:

- **Имя правила**

  Укажите имя нового правила активации.

  Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).

- **Группа администрирования**

  Выберите группу администрирования, в которую будут автоматически перемещаться устройства.

- **Активное правило**

  Если этот параметр включен, правило включено и начинает применяться сразу после сохранения.

  Если этот параметр выключен, правило создается, но оно не включено. Правило не будет работать до тех пор, пока вы не включите этот параметр.

- **Приоритет**

  Вы можете указать приоритет правила перемещения. Самый высокий приоритет равен 1. Чем больше значение **Приоритет**, тем ниже приоритет правила и его позиция в списке.

  Если приоритет не назначен, правилу назначается самый низкий приоритет.

  При копировании правила копии правила присваивается приоритет исходного правила. Приоритет исходного правила увеличивается на 1.

- **Перемещать только устройства, которые не входят ни в одну группу администрирования**

  Если этот параметр включен, только нераспределенные устройства будут перемещены в выбранную группу.

  Если этот параметр выключен, устройства, которые уже принадлежат другим группам администрирования, а также нераспределенные устройства, будут перемещены в выбранную группу.

- **Применить правило**

  Вы можете выбрать один из следующих вариантов:

  - **Выполнять один раз для каждого устройства**

    Правило применяется однократно для каждого устройства, соответствующего указанным критериям.

  - **Выполнять один раз для каждого устройства и при каждой установке Агента администрирования**

    Правило применяется однократно для каждого устройства, соответствующего указанным критериям, а затем только при переустановке Агента администрирования на этих устройствах.

  - **Применять правило постоянно**

    Правило применяется в соответствии с расписанием, автоматически задаваемым на Сервере администрирования (обычно каждые несколько часов).

4. На вкладке **Условия правила** укажите хотя бы один критерий, по которому устройства будут перемещены в группу администрирования.

5. Нажмите на кнопку **Сохранить**.

Правило перемещения создано. Оно появится в списке правил перемещения.

Чем выше положение правила в списке, тем выше его приоритет.

Чтобы изменить приоритет:

1. Установите флажок около правила перемещения.

2. Выполните одно из следующих действий:

   - Нажмите на кнопку **Изменить приоритет** и укажите новый приоритет.

   - Переместите правило вверх или вниз по списку с помощью кнопок **Вверх** или **Вниз**.

3. Нажмите на кнопку **Сохранить**.

> Если выбран параметр **Применять правило постоянно**, правило перемещения применяется независимо от приоритета. Такие правила применяются по расписанию, которое Сервер администрирования устанавливает автоматически.

Если атрибуты устройства удовлетворяют сразу нескольким правилам, то устройство будет перемещено в целевую группу того правила, которое имеет больший приоритет (стоит в списке правил выше).

Копирование правил перемещения устройств

Можно копировать правила перемещения устройств, например, если требуется несколько одинаковых правил для разных целевых групп администрирования.

Чтобы скопировать правило перемещения устройств:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Управление активами → Правила перемещения**.
   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание → Развертывание и назначение → Правила перемещения**.

   Отобразится список правил перемещения устройств.

2. Установите флажок напротив правила, которое требуется скопировать.
3. Нажмите на кнопку **Копировать**.
4. В открывшемся окне при необходимости измените данные на вкладке **Общие** либо оставьте существующие значения, если требуется только скопировать правило, без изменения параметров:

   - **Имя правила**

     Укажите имя нового правила активации.

     Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).

   - **Группа администрирования**

     Выберите группу администрирования, в которую будут автоматически перемещаться устройства.

   - **Активное правило**

     Если этот параметр включен, правило включено и начинает применяться сразу после сохранения.

     Если этот параметр выключен, правило создается, но оно не включено. Правило не будет работать до тех пор, пока вы не включите этот параметр.

   - **Приоритет**

     Вы можете указать приоритет правила перемещения. Самый высокий приоритет равен 1. Чем больше значение **Приоритет**, тем ниже приоритет правила и его позиция в списке.

     Если приоритет не назначен, правилу назначается самый низкий приоритет.

     При копировании правила копии правила присваивается приоритет исходного правила. Приоритет исходного правила увеличивается на 1.

   - **Перемещать только устройства, которые не входят ни в одну группу администрирования**

     Если этот параметр включен, только нераспределенные устройства будут перемещены в выбранную группу.

     Если этот параметр выключен, устройства, которые уже принадлежат другим группам администрирования, а также нераспределенные устройства, будут перемещены в выбранную группу.

- **Применить правило**

  Вы можете выбрать один из следующих вариантов:

  - **Выполнять один раз для каждого устройства**

    Правило применяется однократно для каждого устройства, соответствующего указанным критериям.

  - **Выполнять один раз для каждого устройства и при каждой установке Агента администрирования**

    Правило применяется однократно для каждого устройства, соответствующего указанным критериям, а затем только при переустановке Агента администрирования на этих устройствах.

  - **Применять правило постоянно**

    Правило применяется в соответствии с расписанием, автоматически задаваемым на Сервере администрирования (обычно каждые несколько часов).

5. На вкладке **Условия правила** укажите критерии для устройств, которые требуется переместить автоматически.

6. Нажмите на кнопку **Сохранить**.

Будет создано новое правило перемещения. Оно появится в списке правил перемещения.

Условия для правила перемещения устройств

При создании или копировании правила перемещения клиентских устройств в группы администрирования на вкладке **Условия правила** вы задаете условия перемещения устройств. Чтобы определить, какие устройства следует перемещать, можно использовать следующие критерии:

- Теги, присвоенные клиентским устройствам.
- Параметры сети. Например, вы можете перемещать устройства с IP-адресами из указанного диапазона.
- Управляемые приложения, установленные на клиентских устройствах, например Агент администрирования или Сервер администрирования.
- Виртуальные машины, которые являются клиентскими устройствами.
- Информация об организационном подразделении Active Directory (OU) с клиентскими устройствами.
- Информация об облачном сегменте с клиентскими устройствами.

Ниже вы можете найти описание того, как указать эту информацию в правиле перемещения устройств.

Если в правиле указано несколько условий, срабатывает логический оператор AND и применяются все условия одновременно. Если вы не выберете какие-либо параметры или оставите некоторые поля пустыми, такие условия не применяются.

Вкладка Теги

На этой вкладке можно настроить поиск устройств по ключевым словам (тегам), которые были добавлены ранее в описания клиентских устройств. Для этого выберите необходимые теги. Также вы можете включить следующие параметры:

- **Применить к устройствам без выбранных тегов**

  Если этот параметр включен, все устройства с указанными тегами исключаются из правила перемещения устройств. Если этот параметр выключен, правило перемещения устройств применяется к устройствам со всеми выбранными тегами.

  По умолчанию параметр выключен.

- **Применить, если есть хотя бы один из выбранных тегов**

  Если этот параметр включен, правило перемещения устройств применяется к клиентским устройствам хотя бы с одним из выбранных тегов. Если этот параметр выключен, правило перемещения устройств применяется к устройствам со всеми выбранными тегами.

  По умолчанию параметр выключен.

Вкладка Сеть

На этой вкладке вы можете указать сетевые данные устройств, которые учитывает правило перемещения устройств:

- **Имя устройства в сети Windows**

  Имя устройства в сети Windows (NetBIOS-имя) или IPv4-адрес или IPv6-адрес.

- **Windows-домен**

  Правило перемещения устройств применяется ко всем устройствам, включенным в указанный Windows-домен.

- **DNS-имя устройства**

  DNS-имя домена клиентского устройства, которое вы хотите переместить. Заполните это поле, если в вашей сети есть DNS-сервер.

  > Если для базы данных, которую вы используете для Open Single Management Platform, настроена сортировка с учетом регистра, учитывайте регистр при указании DNS-имени устройства. Иначе правило перемещения устройств не будет работать.

- **DNS-домен**

  Правило перемещения устройств применяется ко всем устройствам, включенным в указанный основной DNS-суффикс. Заполните это поле, если в вашей сети есть DNS-сервер.

- **IP-диапазон**

  Если этот параметр включен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

  По умолчанию параметр выключен.

- **IP-адрес подключения к Серверу администрирования**

  Если этот параметр включен, можно задать IP-адреса, по которым клиентские устройства подключаются к Серверу администрирования. Для этого укажите IP-диапазон, включающий все необходимые IP-адреса.

  По умолчанию параметр выключен.

- **Устройство находится в IP-диапазоне**

  Если этот параметр включен, вы можете выбрать IP-диапазон, который вы ранее добавили в разделе **IP-диапазоны**. Соответствующие устройства должны быть включены в выбранный IP-диапазон.

  По умолчанию параметр выключен.

- **Изменение профиля подключения**

  Выберите одно из следующих значений:

  - **Да**. Правило перемещения устройств применяется только к клиентским устройствам с измененным профилем подключения.
  - **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, профиль подключения которых не изменялся.
  - **Значение не выбрано**. Условие не применяется.

- **Под управлением другого Сервера администрирования**

  Выберите одно из следующих значений:

  - **Да**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым другими Серверами администрирования. Эти Серверы отличаются от Сервера, на котором вы настраиваете правило перемещения устройств.
  - **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым текущим Сервером администрирования.
  - **Значение не выбрано**. Условие не применяется.

Вкладка Приложения

На этой вкладке можно настроить правило перемещения устройств на основе управляемых приложений и операционных систем, установленных на клиентских устройствах:

- **Агент администрирования установлен**

  Выберите одно из следующих значений:

  - **Да**. Правило перемещения устройств применяется только к клиентским устройствам, на которых установлен Агент администрирования.
  - **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, на которых не установлен Агент администрирования.
  - **Значение не выбрано**. Условие не применяется.

- **Приложения**

  Укажите, какие управляемые приложения должны быть установлены на клиентских устройствах, чтобы к этим устройствам применялось правило перемещения устройств. Например, вы можете выбрать **Агент администрирования Kaspersky Security Center 17** или **Сервер администрирования Kaspersky Security Center 17**.

  Если вы не выберете управляемое приложение, условие не будет применяться.

- **Включено**

  Можно выбирать клиентские устройства на основе версии операционной системы. Для этого укажите операционные системы, которые должны быть установлены на клиентских устройствах. В результате правило перемещения устройств применяется к клиентским устройствам с выбранными операционными системами.

  Если этот параметр выключен, условие не применяется. По умолчанию параметр выключен.

- **Архитектура операционной системы**

  Можно выбирать клиентские устройства по разрядности операционной системы. В поле **Архитектура операционной системы** можно выбрать одно из следующих значений:

  - **Нет данных**
  - **x86**
  - **AMD64**
  - **IA64**

  Чтобы проверить какая архитектура используется в операционной системе клиентских устройств:

  1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
  2. Нажмите на кнопку **Параметры столбцов** справа (⚙).
  3. Выберите параметр **Архитектура ОС** и нажмите на кнопку **Сохранить**.

     После этого для каждого управляемого устройства отобразится архитектура операционной системы.

- **ОС менеджера пакетов**

  Клиентские устройства можно выбирать по менеджеру пакетов операционной системы. В поле **ОС менеджера пакетов** можно выбрать одно из следующих значений:

  - rpm – для устройств под управлением операционных систем Red Hat Enterprise Linux, CentOS, Fedora, SUSE, Oracle Linux;
  - apt (dpkg) – для устройств под управлением операционных систем Debian, Ubuntu, Kali;
  - pkg – для устройств под управлением операционных систем FreeBSD, OpenBSD.

  Чтобы проверить какой менеджер пакетов используется в операционной системе клиентских устройств:

  1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
  2. Нажмите на кнопку **Параметры столбцов** справа (⚙).
  3. Выберите пункт **ОС менеджера пакетов**, затем нажмите на кнопку **Сохранить**.

     Для каждого управляемого устройства отображается менеджер пакетов, используемый в его операционной системе.

- **Версия пакета обновления ОС**

  В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- **Пользовательский сертификат**

  Выберите одно из следующих значений:

  - **Установлено**. Правило перемещения устройств применяется только к мобильным устройствам с мобильным сертификатом.
  - **Не установлено**. Правило перемещения устройств применяется только к мобильным устройствам без мобильного сертификата.
  - **Значение не выбрано**. Условие не применяется.

- **Включено**

  > Этот параметр применим только для операционных систем Windows.

  Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить правило перемещения устройств для всех номеров сборки, кроме указанного.

- **Включено**

  > Этот параметр применим только для операционных систем Windows.

Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить правило перемещения устройств для всех номеров сборки, кроме указанного.

Вкладка Виртуальные машины

На этой вкладке можно настроить параметры правила перемещения клиентских устройств в зависимости от того, являются эти устройства виртуальными машинами или частью инфраструктуры виртуальных рабочих столов (VDI):

- **Является виртуальной машиной**

  В раскрывающемся списке можно выбрать одно из следующих значений:

  - **Неизвестно**. Условие не применяется.
  - **Нет**. Перемещаемые устройства не должны являться виртуальными машинами.
  - **Да**. Перемещаемые устройства должны являться виртуальными машинами.

- **Тип виртуальной машины**

- **Часть Virtual Desktop Infrastructure**

  В раскрывающемся списке можно выбрать одно из следующих значений:

  - **Неизвестно**. Условие не применяется.
  - **Нет**. Перемещаемые устройства не должны являться частью VDI.
  - **Да**. Перемещаемые устройства должны являться частью VDI.

Вкладка Контроллеры домена

На этой вкладке вы можете указать, что требуется перемещать устройства, входящие в организационное подразделение домена. Вы также можете перемещать устройства из всех дочерних подразделений указанного подразделения домена:

- **Устройство входит в следующее подразделение**

  Если этот параметр включен, правило перемещения устройств применяется к устройствам из организационного подразделения контроллера домена, указанного в списке под параметром.

  По умолчанию параметр выключен.

- **Включать дочерние подразделения**

  Если этот параметр включен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы контроллера домена.

  По умолчанию параметр выключен.

- **Перемещать устройства из дочерних подразделений в соответствующие подгруппы**

- **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств**
- **Удалять подгруппы, отсутствующие в домене**
- **Устройство включено в следующую группу безопасности домена**

  Если этот параметр включен, правило перемещения устройств применяется к устройствам из доменной группы безопасности, указанной в списке под параметром.

  По умолчанию параметр выключен.

Вкладка Облачные сегменты

На этой вкладке можно указать, что требуется перемещать устройства, которые относятся к определенным облачным сегментам:

- **Устройство находится в облачном сегменте**

  При выборе этого параметра правило перемещения устройств применяется к клиентским устройствам, принадлежащим облачному сегменту. Вы можете выбрать нужный облачный сегмент вплоть до подсети в списке под параметром.

  По умолчанию параметр выключен.

- **Включать дочерние объекты**

  При выборе этого параметра правило перемещения устройств применяется не только к выбранному облачному сегменту, но и к дочерним объектам этого сегмента.

  По умолчанию параметр выключен.

- **Перемещать устройства в соответствующие подгруппы**
- **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств**
- **Удалять подгруппы, для которых нет соответствия в облачных сегментах**
- **Устройство обнаружено с помощью API**

  В раскрывающемся списке можно выбрать, обнаруживается ли устройство средствами API:

  - **AWS**. Устройство обнаружено с использованием AWS API, то есть устройство находится в облачном окружении AWS.
  - **Azure**. Устройство обнаружено с использованием Azure API, то есть устройство находится в облачном окружении Azure.
  - **Google Cloud.** Устройство обнаружено с использованием Google API, то есть устройство находится в облачном окружении Google Cloud.
  - **Нет**. Устройство не обнаруживается с помощью AWS, Azure или Google API, то есть оно либо находится вне облачного окружения, либо находится в облачном окружении, но недоступно для поиска с помощью API.
  - **Не задано**. Это условие не применяется.

Добавление устройств в состав группы администрирования вручную

Вы можете перемещать устройства в группы администрирования автоматически, создавая правила перемещения устройств, или вручную, перемещая устройства из одной группы администрирования в другую, или добавляя устройства в выбранную группу администрирования. В этом разделе описано, как вручную добавить устройства в группу администрирования.

Чтобы вручную добавить одно или несколько устройств в состав выбранной группы администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
2. Выберите группу администрирования, в которую вы хотите добавить устройства:
   - Для корневой группы:

     В этом случае вы можете перейти к следующему шагу.
   - Для подгруппы:

     Нажмите на кнопку **Показать иерархию** в верхней части страницы и в открывшемся окне нажмите на имя подгруппы.

     Путь к выбранной группе отображается в верхней части страницы. Чтобы перейти к группе администрирования, нажмите на ссылку с названием группы. По умолчанию последняя ссылка в пути неактивна. Также вы можете закрыть окно иерархии, нажав на кнопку **Скрыть иерархию**.
3. Нажмите на кнопку **Добавить устройства**.

   В результате запустится мастер перемещения устройств.
4. Составьте список устройств, которые вы хотите добавить в группу администрирования.

   > В список устройств могут быть добавлены только те устройства, информация о которых уже была добавлена в базу данных Сервера администрирования при подключении устройства или в результате обнаружения устройств.

   Выберите, как вы хотите добавить устройства в список:

   - Нажмите на кнопку **Добавить устройства** и укажите устройства одним из следующих способов:
     - Выберите устройства из списка устройств, обнаруженных Сервером администрирования.
     - Укажите IP-адреса устройств или IP-диапазон.

       > IP-диапазон не должен содержать более 1 048 576 адресов.

- Укажите NetBIOS-имя устройства или DNS-имя.

  Поле с именем устройства не должно содержать пробелы, отступы, а также следующие запрещенные символы: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

- Нажмите на кнопку **Импортировать устройства из файла**, чтобы импортировать список устройств из файла формата TXT. Каждый адрес устройства (или имя устройства) должен располагаться в отдельной строке.

  Файл не должен содержать пробелы, отступы, а также следующие запрещенные символы: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

5. Просмотрите список устройств, которые будут добавлены в группу администрирования. Вы можете редактировать список, добавляя или удаляя устройства.

6. После того как вы убедитесь, что в списке нет ошибок, нажмите на кнопку **Далее**.

Мастер обрабатывает список устройств и отображает результат. После завершения работы мастера выбранные устройства включаются в состав группы администрирования и отображаются в списке устройств под именами, установленными для них Сервером администрирования.

Перемещение устройств или кластеров в состав группы администрирования вручную

Устройства можно перемещать из одной группы администрирования в другую или из группы нераспределенных устройств в группу администрирования.

Также можно перемещать кластеры или массивы серверов из одной группы администрирования в другую. При перемещении кластера или массива серверов в другую группу, все его узлы перемещаются вместе с ним, так как кластер и любой из его узлов всегда принадлежат к одной группе администрирования. При выборе одного узла кластера на вкладке **Устройства**, кнопка **Переместить в группу** становится недоступной.

Чтобы переместить одно или несколько устройств или кластеров в состав выбранной группы администрирования:

1. Откройте группу администрирования, в которую вы хотите переместить устройства. Для этого выполните одно из следующих действий:

   - Чтобы открыть группу администрирования, в главном меню перейдите в раздел **Управление активами** → **Управляемые устройства** и выберите нужную группу администрирования.

     - Для корневой группы вы можете перейти к следующему шагу.

     - Для подгруппы в верхней части страницы нажмите на кнопку **Показать иерархию** и в открывшемся окне выберите нужную группу администрирования.

   - Чтобы открыть группу **Нераспределенные устройства**, в главном меню перейдите в раздел **Управление активами** → **Нераспределенные устройства**.

2. Если группа администрирования содержит кластеры или массивы серверов, раздел **Управляемые устройства** разделен на две вкладки – **Устройства** и **Кластеры и массивы серверов**. Откройте вкладку объекта, который хотите переместить.

3. Установите флажки рядом с устройствами или кластерами, которые требуется переместить в другую группу.

4. Нажмите на кнопку **Переместить в группу**.

5. В иерархии групп администрирования установите флажок рядом с группой администрирования, в которую вы хотите переместить выбранные устройства или кластеры.

6. Нажмите на кнопку **Переместить**.

Выбранные устройства или кластеры перемещаются в выбранную группу администрирования.

Настройка правил хранения для нераспределенных устройств

После того как опрос сети Windows завершен, обнаруженные устройства помещаются в подгруппы группы администрирования Нераспределенные устройства. Эта группа администрирования находится по следующему пути: **Обнаружение устройств и развертывание → Обнаружение устройств → Windows-домены**. Папка **Windows-домены** является родительской группой. Папка содержит дочерние группы, имена которых соответствуют доменам и рабочим группам, обнаруженным во время опроса. Родительская группа может также содержать группы администрирования мобильных устройств. Вы можете настроить правила хранения нераспределенных устройств для родительской группы администрирования и для каждой дочерней группы. Правила хранения не зависят от параметров обнаружения устройств и работают, даже если обнаружение устройств выключено.

Правила хранения устройств не влияют на устройства, на которых один или несколько дисков зашифрованы с помощью полнодискового шифрования. Такие устройства не удаляются автоматически – вы можете удалить их только вручную. Если вам нужно удалить устройство с зашифрованным жестким диском, сначала расшифруйте диск, а затем удалите устройство.

Чтобы настроить правила хранения нераспределенных устройств:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание → Обнаружение устройств → Windows-домены**.

2. Выполните одно из следующих действий:

   - Чтобы настроить параметры родительской группы, нажмите на кнопку **Свойства**.

     Откроется окно свойств Windows-домена.

   - Чтобы настроить параметры дочерней группы, нажмите на ее имя.

     Откроется окно свойств дочерней группы.

3. Настройте следующие параметры:

   - **Удалять устройство из группы, если оно неактивно больше (сут)**

     Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. По умолчанию этот параметр распространяется на дочерние группы. Временной интервал, установленный по умолчанию, составляет 7 дней.

По умолчанию параметр включен.

- **Наследовать из родительской группы**

  Если этот параметр включен, период хранения для устройств в текущей группе наследуется от родительской группы и не может быть изменен.

  Этот параметр доступен только для дочерних групп.

  По умолчанию параметр включен.

- **Обеспечить принудительное наследование для дочерних групп**

  Значения параметров будут распределены по дочерним группам, но в свойствах дочерних групп эти параметры недоступны для изменений.

  По умолчанию параметр выключен.

4. Нажмите на кнопку **Принять**.

Ваши изменения сохранены и применены.

Инвентаризация оборудования

Список оборудования (**Управление активами** → **Оборудование**), который вы используете для инвентаризации оборудования, заполняется двумя способами: автоматически и вручную. После каждого опроса сети все обнаруженные устройства автоматически добавляются в список; однако вы также можете добавить устройства вручную, если не хотите опрашивать сеть. Вы можете добавить другие устройства в список вручную, например, маршрутизаторы, принтеры или оборудование.

В свойствах устройства можно просматривать и редактировать подробную информацию об устройствах.

В списке оборудования могут присутствовать следующие типы устройств:

- компьютеры;
- мобильные устройства;
- сетевые устройства;
- виртуальные устройства;
- компьютерные комплектующие;
- компьютерная периферия;
- подключаемые устройства;
- VoIP-телефоны;
- сетевые хранилища.

Администратор может присваивать обнаруженным устройствам признак *Корпоративное оборудование*. Этот признак можно присвоить в свойствах устройства вручную или задать критерии для его автоматического присвоения. В этом случае признак *Корпоративное оборудование* присваивается по типу устройства.

Kaspersky SIEM Cloud позволяет выполнять списание оборудования. Для этого в свойствах устройства необходимо выбрать параметр **Списано**. Такое устройство не отображается в списке оборудования.

Администратор может работать со списком программируемых логических контроллеров (ПЛК) в папке **Оборудование**. Подробная информация о работе со списками ПЛК приведена в *Руководстве пользователя Kaspersky Industrial CyberSecurity for Nodes*.

Добавление информации о новых устройствах

Чтобы добавить информацию о новых устройствах в сети:

1. В главном окне приложения перейдите в раздел **Управление активами → Оборудование**.
2. Нажмите на кнопку **Добавить**, чтобы открыть окно **Новое устройство**.
3. В окне **Новое устройство** в раскрывающемся списке **Тип устройства** выберите тип устройства, которое вы хотите добавить.
4. Нажмите на кнопку **OK**.

   Откроется окно свойств устройства на разделе **Общие**.
5. В разделе **Общие** заполните поля ввода данными об устройстве. В разделе **Общие** доступны следующие параметры:

   - **Корпоративное устройство**. Установите флажок, если вы хотите присвоить устройству признак *Корпоративное*. По этому признаку можно выполнять поиск устройств в папке **Оборудование**.
   - **Списано**. Установите флажок, если вы не хотите, чтобы устройство отображалось в списке устройств в папке **Оборудование**.
6. Нажмите на кнопку **Применить**.

Новое устройство отобразится в рабочей области страницы **Оборудование**.

Настройка критериев определения корпоративных устройств

Чтобы настроить критерии определения корпоративных устройств:

1. В главном окне приложения перейдите в раздел **Управление активами → Оборудование**.
2. В верхней части страницы **Оборудование** нажмите на ссылку **Настроить критерии определения корпоративных устройств**.

   Откроется панель **Настроить критерии определения корпоративных устройств**.

3. В панели **Настроить критерии определения корпоративных устройств** включите параметр **Автоматически устанавливать для устройства признак "Корпоративное"**. Укажите типы устройств, которым атрибут *Корпоративное* назначается автоматически.

   Этот параметр влияет только на те устройства, которые были добавлены с помощью опроса сети. Для устройств, добавленных вручную, установите параметр *Корпоративное* вручную.

4. Нажмите на кнопку **OK**.

Критерии обнаружения корпоративных устройств настроены.

Настройка приложений "Лаборатории Касперского"

В этом разделе содержится информация о настройке вручную политик и задач, о ролях пользователей, о построении структуры групп администрирования и об иерархии задач.

Сценарий: настройка защиты сети

Мастер первоначальной настройки создает политики и задачи с параметрами по умолчанию. Эти параметры могут оказаться не оптимальными или даже запрещенными в организации. Поэтому рекомендуется настроить эти политики и задачи и создать дополнительные политики и задачи, если это необходимо для вашей сети.

Предварительные требования

Убедитесь, что вы успешно завершили основной сценарий первоначальной настройки Open Single Management Platform, включая мастер первоначальной настройки.

Во время работы мастера первоначальной настройки в корневой группе администрирования **Управляемые устройства** создаются следующие политики и задачи:

- политика Kaspersky Endpoint Security;
- групповая задача обновления Kaspersky Endpoint Security;
- политика Агента администрирования;
- Поиск уязвимостей и требуемых обновлений (задача Агента администрирования).

Этапы

Настройка защиты сети состоит из следующих этапов:

1. **Настройка и распространение политик и профилей политик для приложений "Лаборатории Касперского"**

   Для настройки и распространения параметров приложений "Лаборатории Касперского", установленных на управляемых устройствах, можно использовать два различных подхода управления безопасностью: ориентированный на пользователей и ориентированный на устройства. Также вы можете комбинировать эти два подхода.

2. **Настройка задач для удаленного управления приложениями "Лаборатории Касперского"**

   Проверьте задачи, созданные с помощью мастера первоначальной настройки, и при необходимости оптимизируйте их параметры.

   Инструкции:

   - Настройка групповой задачи обновления Kaspersky Endpoint Security.
   - Создание задачи *Поиск уязвимостей и требуемых обновлений.*

   При необходимости создайте дополнительные задачи управления приложениями "Лаборатории Касперского", установленными на клиентских устройствах.

3. **Оценка и ограничение загрузки событий в базу данных**

   Информация о событиях, которые возникают во время работы управляемых приложений, передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

   Инструкции: Настройка количества событий в хранилище событий.

4. **Оптимизация нагрузки на приложения для защиты конечных точек**

   Чтобы избежать снижение производительности оптимизируйте потребление ресурсов приложениями для защиты конечных точек.

   Подробные инструкции см. в:

   Справка Kaspersky Endpoint Security for Windows

   Справка Kaspersky Endpoint Security for Linux

Результаты

После завершения этого сценария ваша сеть будет защищена благодаря настройке приложений "Лаборатории Касперского", задач и событий, получаемых Сервером администрирования:

- приложения "Лаборатории Касперского" настроены в соответствии с политиками и профилями политик.
- Управление приложениями осуществляется с помощью набора задач.
- Задано максимальное количество событий, которые могут храниться в базе данных.

После завершения настройки защиты сети вы можете приступить к настройке регулярных обновлений баз и приложений "Лаборатории Касперского".

Подходы к управлению безопасностью, ориентированные на устройства и на пользователей

Вы можете управлять параметрами безопасности с позиции функций устройства и с позиции пользовательских ролей. Первый подход называется *управление безопасностью, ориентированное на устройства*, второй подход называется *управление безопасностью, ориентированное на пользователей*. Чтобы применить разные параметры приложений к разным устройствам, вы можете использовать один или оба типа управления в комбинации.

Управление безопасностью, ориентированное на устройства, позволяет вам применять различные параметры приложения безопасности к управляемым устройствам в зависимости от особенностей устройства. Например, вы можете применить различные параметры к устройствам, которые размещены в разных группах администрирования. Вы также можете разграничить устройства по использованию этих устройств в Active Directory или по характеристикам аппаратного обеспечения.

Управление безопасностью, ориентированное на пользователя, позволяет вам применять различные параметры приложений безопасности к различным ролям пользователей. Вы можете создать несколько пользовательских ролей, назначить соответствующую пользовательскую роль каждому пользователю и определить различные параметры приложения для устройств, принадлежащих пользователям с различными ролями. Например, можно применить различные параметры приложений к устройствам бухгалтеров и к устройствам специалистов отдела кадров. В результате внедрения управления безопасностью, ориентированного на пользователей, каждый отдел – отдел бухгалтерии и отдел кадров – получит свою собственную конфигурацию параметров для работы с приложениями "Лаборатории Касперского". Конфигурация параметров определяет, какие параметры приложения могут быть изменены пользователями, а какие принудительно установлены и заблокированы администратором.

Управление безопасностью, ориентированное на пользователей, позволяет применять заданные параметры приложений для отдельных пользователей. Это может потребоваться, если сотруднику назначена уникальная роль в организации или если требуется проконтролировать проблемы безопасности, связанные с определенным сотрудником. В зависимости от роли этого сотрудника в компании, можно расширить или сократить его права, чтобы изменить параметры приложения. Например, может потребоваться расширить права системного администратора, управляющего клиентскими устройствами в локальном офисе.

Вы также можете комбинировать подходы к управлению безопасностью, ориентированные на пользователей и ориентированные на устройства. Например, можно настроить разные политики для каждой группы администрирования, а затем дополнительно создать профили политик для одной или нескольких пользовательских ролей вашей организации. В этом случае политики и профили политик применяются в следующем порядке:

1. Применяются политики, созданные для управления безопасностью, ориентированного на устройства.
2. Они модифицируются профилями политик в соответствии с приоритетами профилей политик.
3. Политики модифицируются профилями политик, связанными с ролями пользователей.

Настройка и распространение политик: подход, ориентированный на устройства

В этом разделе приведен сценарий, ориентированный на устройства, для централизованной настройки приложений "Лаборатории Касперского", установленных на управляемых устройствах. После завершения этого сценария приложения будут настроены на всех управляемых устройствах в соответствии с политиками приложений и профилями политики, которые вы определяете.

Возможно, вы также захотите рассмотреть управление безопасностью, ориентированное на пользователей как альтернативу или дополнительную возможность для подхода, ориентированного на устройства.

Процесс

Сценарий управления приложениями "Лаборатории Касперского", ориентированный на устройства, содержит следующие шаги:

1. **Настройка политик приложений**

   Настройте параметры установленных приложений "Лаборатории Касперского" на управляемых устройствах с помощью создания политики для каждого приложения. Этот набор политик будет применен к клиентским устройствам.

   При настройке защиты сети с помощью мастера первоначальной настройки Open Single Management Platform создает политику по умолчанию для Kaspersky Endpoint Security для Windows. Если вы завершили процесс настройки с помощью этого мастера, вам не нужно создавать политику для этого приложения. Перейдите к настройке политики Kaspersky Endpoint Security вручную.

   Если у вас иерархическая структура нескольких групп администрирования, дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики. Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик позволяет эффективно управлять устройствами в группах администрирования.

   Инструкция: Создание политики.

2. **Создание профилей политики (если требуется)**

   Если вы хотите, чтобы к устройствам из одной группы администрирования применялись разные параметры политики, создайте профили политики для этих устройств. Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на управляемом устройстве.

   Используя условия активации профиля, вы можете применять различные профили политики, например, к устройствам, расположенным в определенном подразделении или группе безопасности Active Directory, имеющим определенную конфигурацию программного обеспечения или имеющим заданные теги. Используйте теги для фильтрации устройств, соответствующих определенным критериям. Например, вы можете создать тег *Windows*, назначить его всем устройствам под управлением операционной системы Windows, а затем указать этот тег в правилах активации профиля политики. В результате на устройствах под управлением операционной системы Windows установленные приложения "Лаборатории Касперского" будут управляться своим профилем политики.

Инструкции:

- Создание профиля политики.
- Создание правила активации профиля политики.

3. **Распространение политик и профилей политик на управляемые устройства**

   Open Single Management Platform автоматически синхронизирует Сервер администрирования с управляемыми устройствами несколько раз в час. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно. После завершения синхронизации политики и профили политик доставляются и применяются к установленным приложениям "Лаборатории Касперского".

   Вы можете проверить, доставлены ли политики и профили политик на устройство. Open Single Management Platform определяет дату и время доставки в свойствах устройства.

   Инструкции: Принудительная синхронизация

Результаты

После завершения сценария, ориентированного на устройства, приложения "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик.

Политики приложений и профили политик будут автоматически применяться к новым устройствам, добавленным в группы администрирования.

Настройка и распространение политик: подход, ориентированный на пользователя

В этом разделе описывается сценарий, ориентированный на пользователя для централизованной настройке приложений "Лаборатории Касперского", установленных на управляемых устройствах. После завершения этого сценария приложения будут настроены на всех управляемых устройствах в соответствии с политиками приложений и профилями политики, которые вы определяете.

Возможно, вы также захотите рассмотреть управление безопасностью, ориентированное на устройства как альтернативу или дополнительную возможность для подхода, ориентированного на пользователя. Узнайте больше о двух подходах к управлению.

Процесс

Сценарий управления приложениями "Лаборатории Касперского", ориентированный на пользователя, содержит следующие шаги:

1. **Настройка политик приложений**

   Настройте параметры установленных приложений "Лаборатории Касперского" на управляемых устройствах с помощью создания политики для каждого приложения. Этот набор политик будет применен к клиентским устройствам.

При настройке защиты сети с помощью мастера первоначальной настройки Open Single Management Platform создает политику по умолчанию для Kaspersky Endpoint Security. Если вы завершили процесс настройки с помощью этого мастера, вам не нужно создавать политику для этого приложения. Перейдите к настройке политики Kaspersky Endpoint Security вручную.

Если у вас иерархическая структура нескольких групп администрирования, дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики. Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик позволяет эффективно управлять устройствами в группах администрирования.

Инструкция: Создание политики.

2. **Укажите пользователей в качестве владельцев устройств**

   Назначьте управляемым устройствам соответствующих пользователей.

   Инструкция: Назначение пользователя владельцем устройства.

3. **Определение пользовательских ролей, типичных для вашей организации**

   Подумайте о различных видах работ, которые обычно выполняют сотрудники вашей организации. Вам нужно разделить всех сотрудников в соответствии с их ролями. Например, вы можете разделить их по отделам, профессиям или должностям. После этого вам потребуется создать роль пользователя для каждой группы. В этом случае каждая пользовательская роль будет иметь свой собственный профиль политики, содержащий параметры приложения, специфичные для этой роли.

4. **Создание пользовательских ролей**

   Создайте и настройте пользовательскую роль для каждой группы сотрудников, которую вы определили на предыдущем шаге, или используйте предопределенные роли. Роли пользователей содержат набор прав доступа к функциям приложения.

   Инструкция: Создание роли пользователя.

5. **Определение области для каждой роли пользователя**

   Для каждой созданной роли пользователя определите пользователей и/или группы безопасности и группы администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

   Инструкция: Изменение области для роли пользователя.

6. **Создание профилей политики**

   Создайте профиль политики для каждой роли пользователя вашей организации. Профили политики определяют, какие параметры должны применяться к приложениям, установленным на устройствах пользователей, в зависимости от роли каждого пользователя.

   Инструкция: Создание профиля политики.

7. **Связь профиля политики с ролями пользователей**

   Свяжите созданные профили политики с ролями пользователей. После чего, профиль политики становится активным для пользователей, которым определена эта роль. Параметры профиля политики, применяются к приложениям "Лаборатории Касперского", установленным на устройствах пользователя.

   Инструкция: Связь профилей политики с ролями.

8. **Распространение политик и профилей политик на управляемые устройства**

Open Single Management Platform автоматически синхронизирует Сервер администрирования с управляемыми устройствами несколько раз в час. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно. После завершения синхронизации политики и профили политик доставляются и применяются к установленным приложениям "Лаборатории Касперского".

Вы можете проверить, доставлены ли политики и профили политик на устройство. Open Single Management Platform определяет дату и время доставки в свойствах устройства.

Инструкции: Принудительная синхронизация

Результаты

После завершения сценария, ориентированного на пользователя, приложения "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик и профили политик.

Для нового пользователя вам необходимо создать учетную запись, назначить пользователю одну из созданных пользовательских ролей и назначить устройства пользователю. Политики приложений и профили политик будут автоматически применяться к устройствам этого пользователя.

Параметры политики Агента администрирования

Чтобы настроить параметры политики Агента администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на название политики Агента администрирования.

   Откроется окно свойств политики Агента администрирования.

См. таблицу сравнения, в которой подробно описано как применяются параметры, приведенные ниже, в зависимости от используемой операционной системы.

Вкладка Общие

На этой вкладке можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
  - **Активна**
  - **Неактивна**

    Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.

- В блоке **Наследование параметров** можно настроить параметры наследования политики:

  - **Наследовать параметры родительской политики**

    Если параметр включен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

    По умолчанию параметр включен.

  - **Обеспечить принудительное наследование параметров для дочерних политик**

    Если параметр включен, после применения изменений в политике будут выполнены следующие действия:

    - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;

    - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически включен параметр **Наследовать параметры родительской политики**.

    Когда параметр включен, значения параметров дочерних политик недоступны для изменения.

    По умолчанию параметр выключен.

Вкладка Настройка событий

На этой вкладке можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности в следующих разделах на вкладке **Настройка событий**:

- **Отказ функционирования**
- **Предупреждение**
- **Информационное сообщение**

В каждом разделе в списке типов событий отображаются названия событий и время хранения событий на Сервере администрирования по умолчанию (в днях). По кнопке **Свойства** можно настроить параметры регистрации и уведомления о событиях, выбранных в списке. По умолчанию общие настройки уведомлений, указанные для всего Сервера администрирования, используются для всех типов событий. Однако можно изменить определенные параметры для заданных типов событий.

Вкладка Параметры приложения

Параметры

В разделе **Параметры** можно настроить параметры политики Агента администрирования:

- **Распространять файлы только через точки распространения**

  Если этот параметр включен, Агенты администрирования на управляемых устройствах получают обновления только от точек распространения.

Если этот параметр выключен, Агенты администрирования на управляемых устройствах получают обновления от точек распространения или от Сервера администрирования.

> Обратите внимание, что приложения безопасности на управляемых устройствах получают обновления от источника, заданного в задаче обновления для каждого приложения безопасности. Если вы включили параметр **Распространять файлы только через точки распространения**, убедитесь, что Open Single Management Platform установлен в качестве источника обновлений в задачах обновления.

По умолчанию параметр выключен.

- **Максимальный размер очереди событий (МБ)**

- **Приложение может получать расширенные данные политики на устройстве**

  Агент администрирования, установленный на управляемом устройстве, передает информацию о применяемой политике в приложение безопасности (например, Kaspersky Endpoint Security for Linux). Передаваемая информация отображается в интерфейсе приложения безопасности.

  Агент администрирования передает следующую информацию:

  - время доставки политики на управляемое устройство;
  - имя активной политики в момент доставки политики на управляемое устройство;
  - название политики для автономных пользователей в момент доставки политики на управляемое устройство (недоступно для Агента администрирования для Linux);
  - имя и полный путь группы администрирования, которой принадлежит управляемое устройство на момент доставки политики на управляемое устройство;
  - список активных профилей политик с указанием их названий и приоритетов на момент доставки политики на управляемое устройство.

  Вы можете использовать эту информацию, чтобы обеспечить применение правильной политики к устройству и в целях устранения неполадок. По умолчанию параметр выключен.

- **Защитить службу Агента администрирования от неавторизованного удаления, остановки или изменения параметров работы**

  Если этот параметр включен, после того, как Агент администрирования был установлен на управляемом устройстве, компонент не может быть удален или изменен без требуемых прав. Работа Агента администрирования не может быть остановлена. Этот параметр не влияет на контроллеры домена.

  Включите этот параметр, чтобы защитить Агент администрирования на рабочих станциях, управляемых с правами локального администратора.

  По умолчанию параметр выключен.

- **Использовать пароль деинсталляции**

  Если параметр включен, при нажатии на кнопку **Изменить** можно указать пароль для утилиты klmover и задачи удаленной деинсталляции Агента администрирования на устройствах с операционной системой Windows.

  По умолчанию параметр выключен.

Хранилища

В разделе **Хранилища** можно выбрать типы объектов, информацию о которых Агент администрирования будет отправлять на Сервер администрирования. Если в политике Агента администрирования наложен запрет на изменение параметров, указанных в этом разделе, эти параметры недоступны для изменения.

- **Информация об установленных приложениях**
- **Включить информацию о патчах**

  Информация о патчах приложений, установленных на клиентских устройствах, отправляется на Сервер администрирования. Включение этого параметра может увеличить нагрузку на Сервер администрирования и СУБД, а также вызвать увеличение объема базы данных.

  По умолчанию параметр включен. Доступен только для Windows.

- **Информация об обновлениях Центра обновления Windows**

  Если параметр установлен, на Сервер администрирования отправляется информация об обязательных обновлениях Центра обновления Windows, которые необходимо установить на клиентских устройствах.

  По умолчанию параметр включен. Доступен только для Windows.

  Информация о необязательных обновлениях Microsoft Windows не отправляется на Сервер администрирования.

- **Информация об уязвимостях в приложениях и соответствующих обновлениях**

  Если этот параметр включен, информация об уязвимостях в приложениях сторонних производителей (включая программное обеспечение Microsoft), обнаруженных на управляемых устройствах, и об обновлениях программного обеспечения для закрытия уязвимостей (не включая программное обеспечение Microsoft) отправляется на Сервер администрирования.

  Выбор этого параметра (**Информация об уязвимостях в приложениях и соответствующих обновлениях**) увеличивает нагрузку на сеть, загрузку диска Сервера администрирования и потребление ресурсов Агентом администрирования.

  По умолчанию параметр включен. Доступен только для Windows.

  Для управления обновлениями приложений Microsoft используйте параметр **Информация об обновлениях Центра обновления Windows**.

- **Информация о реестре оборудования**

Обновления и уязвимости в приложениях

В разделе **Обновления и уязвимости в приложениях** можно настроить поиск и распространение обновлений Windows, а также включить проверку исполняемых файлов на наличие уязвимостей:

- В блоке параметров **Режим поиска Центра обновления Windows** можно выбрать режим поиска обновлений:

  - **Активный**

    Если выбран этот вариант, Сервер администрирования с помощью Агента администрирования инициирует обращение агента обновлений Windows на клиентском устройстве к источнику обновлений: Windows Update Servers или WSUS. Далее Агент администрирования передает на Сервер администрирования информацию, полученную от Агента Центра обновления Windows.

    Этот параметр применяется, только если включен параметр **Соединяться с сервером обновлений для актуализации данных** задачи *Поиск уязвимостей и требуемых обновлений*.

    По умолчанию выбран этот вариант.

  - **Пассивный**

    Если выбран этот вариант, Агент администрирования периодически передает на Сервер администрирования информацию об обновлениях, полученную при последней синхронизации агента обновлений Windows с источником обновления. Если синхронизация агента обновлений Windows с источником обновления не выполняется, данные об обновлениях на Сервере администрирования устаревают.

    Выберите этот параметр, если вы хотите получать обновления из кеша источника обновлений.

  - **Выключен**

    Если выбран этот вариант, Сервер администрирования не запрашивает информацию об обновлениях.

    Выберите этот параметр, если, например, вы хотите сначала протестировать обновления на локальном устройстве.

- **Проверять исполняемые файлы на наличие уязвимостей при запуске**

  Если параметр включен, при запуске исполняемых файлов выполняется их проверка на наличие уязвимостей.

  По умолчанию параметр включен.

Управление перезагрузкой

В разделе **Управление перезагрузкой** можно выбрать и настроить действие, если во время работы, установки или удаления приложения требуется перезагрузить операционную систему управляемого устройства:

- **Не перезагружать операционную систему**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **При необходимости перезагрузить операционную систему автоматически**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

  - **Повторять запрос периодически через (мин)**

    Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

    По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

    Если параметр выключен, предложение перезагрузки отображается только один раз.

  - **Принудительно перезагружать через (мин)**

    После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

    По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать приложения в заблокированных сеансах**

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

Совместный доступ к рабочему столу Windows

В разделе **Совместный доступ к рабочему столу Windows** можно включить и настроить аудит действий администратора на удаленном устройстве пользователя при использовании общего доступа к рабочему столу. Параметры раздела **Совместный доступ к рабочему столу Windows** доступны только для устройств под управлением Windows:

- **Включить аудит**

  Если параметр включен, аудит действий администратора на удаленном устройстве включен. Записи о действиях администратора на удаленном устройстве сохраняются:

  - в журнале событий на удаленном устройстве;
  - в файле с расширением syslog, который находится в папке установки Агента администрирования на удаленном устройстве;
  - в базе событий Kaspersky SIEM Cloud.

  Аудит действий администратора доступен при выполнении следующих условий:

  - лицензия на Системное администрирование уже используется;
  - у администратора есть право на запуск общего доступа к рабочему столу удаленного устройства.

  Если параметр выключен, аудит действий администратора на удаленном устройстве выключен.

  По умолчанию параметр выключен.

- **Маски файлов, чтение которых нужно отслеживать**

  В списке содержатся маски файлов. Когда аудит включен, приложение отслеживает чтение администратором файлов, соответствующих маскам, и сохраняет информацию о чтении файлов. Список доступен, когда установлен флажок **Включить аудит**. Можно изменять маски файлов и добавлять в список новые маски. Новые маски файлов нужно указывать в списке с новой строки.

  По умолчанию указаны маски файлов *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Маски файлов, изменение которых нужно отслеживать**

  В списке содержатся маски файлов на удаленном устройстве. Когда аудит включен, приложение отслеживает изменение администратором файлов, соответствующих маскам, и сохраняет информацию об изменении файлов. Список доступен, когда установлен флажок **Включить аудит**. Можно изменять маски файлов и добавлять в список новые маски. Новые маски файлов нужно указывать в списке с новой строки.

  По умолчанию указаны маски файлов *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Управление патчами и обновлениями

В разделе **Управление патчами и обновлениями** можно настроить получение и распространение обновлений и установку патчей на управляемые устройства: включить или выключить параметр **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**.

Подключения

Раздел **Подключения** включает три вложенных раздела:

- **Сеть**
- **Профили соединений**
- **Расписание соединений**

В разделе **Сеть** можно настроить параметры подключения к Серверу администрирования, включить возможность использования UDP-порта и указать его номер.

- В блоке **Подключение к Серверу администрирования** можно настроить параметры подключения к Серверу администрирования и указать период синхронизации клиентских устройств с Сервером администрирования:
  - **Сжимать сетевой трафик**

    Если параметр выключен, будет увеличена скорость передачи данных Агентом администрирования, сокращен объем передаваемой информации и уменьшена нагрузка на Сервер администрирования.

    > Нагрузка на центральный процессор клиентского компьютера может возрасти.

    По умолчанию флажок установлен.
  - **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**

    Если параметр включен, порты, необходимые для работы Агента администрирования, будут добавлены в список исключений брандмауэра Microsoft Windows.

    По умолчанию параметр включен.
  - **Использовать шлюз соединения точки распространения (при наличии) в параметрах подключения по умолчанию**

    Если параметр включен, то используется шлюз соединений точки распространения, параметры которой заданы в свойствах группы администрирования.

    По умолчанию параметр включен.

- **Использовать UDP-порт**

  Чтобы Агент администрирования подключался к Серверу администрирования через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **Номер UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к Серверу администрирования выполняется через UDP-порт 15000.

- **Номер UDP-порта**

  В поле можно ввести номер UDP-порта. По умолчанию установлен порт 15000.

  Используется десятичная форма записи.

- **Использовать точку распространения для принудительного подключения к Серверу**

  Выберите этот параметр, если вы выбрали параметр **Использовать эту точку распространения в качестве push-сервера** в окне параметров точки распространения. Иначе точка распространения не будет выполнять роль push-сервера.

В подраздел **Профили соединений** новые элементы не могут быть добавлены в список **Профили подключения к Серверу администрирования**, так как кнопка **Добавить** неактивна. Предустановленные профили соединений тоже невозможно изменить.

В разделе **Расписание соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования:

- **Подключаться при необходимости**

- **Подключаться в указанные периоды**

В разделе **Расписание соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования:

- **Подключаться при необходимости**

  Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту администрирования нужно передать данные на Сервер администрирования.

  По умолчанию выбран этот вариант.

- **Подключаться в указанные периоды**

  Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

Опрос сети точками распространения

В разделе **Опрос сети точками распространения** вы можете настроить автоматический опрос сети. Параметры опроса сети доступны только для устройств под управлением Windows. Вы можете использовать следующие параметры, чтобы включить опрос и настроить его расписание:

- **Сеть Windows**

  Параметр доступен только для точек распространения с операционной системой Windows.

Если этот параметр включен, Сервер администрирования автоматически опрашивает сеть в соответствии с расписанием, настроенным по ссылкам **Настроить расписание быстрого опроса** и **Настроить расписание полного опроса**.

Если этот параметр выключен, Сервер администрирования опрашивает сеть с указанным периодом в поле **Период опроса сети (мин)**.

Период обнаружения устройств для Агента администрирования можно настроить в полях **Период опроса Windows-доменов (мин)** (для быстрого опроса сети Windows) и **Период опроса сети (мин)** (для полного опроса сети Windows).

По умолчанию параметр выключен.

- **IP-диапазоны**

  Если этот параметр включен, точка распространения автоматически опрашивает IP-диапазоны в соответствии с расписанием, настроенным по кнопке **Настроить расписание опроса**.

  Если параметр выключен, точка распространения не выполняет опрос IP-диапазонов.

  Периодичность опроса IP-диапазонов для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если параметр включен.

  По умолчанию параметр выключен.

- **Контроллеры доменов**

  Если этот параметр включен, точка распространения автоматически выполняет опрос контроллеров домена в соответствии с расписанием, настроенным по кнопке **Настроить расписание опроса**.

  Если параметр выключен, точка распространения не выполняет опрос контроллеров домена.

  Периодичность опроса контроллеров домена для версий Агента администрирования ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если этот параметр включен.

  По умолчанию параметр выключен.

Параметры сети для точек распространения

В разделе **Параметры сети для точек распространения** вы можете указать параметры доступа к интернету:

- **Использовать прокси-сервер**

  Если этот параметр включен, для подключения точек распространения к серверу обновлений "Лаборатории Касперского" используется прокси-сервер в интернете.

- **Адрес**

- **Номер порта**

- **Не использовать прокси-сервер для локальных адресов**

  Если параметр включен, то при подключении к устройствам в локальной сети не используется прокси-сервер.

  По умолчанию параметр выключен.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  По умолчанию флажок снят.

- **Имя пользователя**

- **Пароль**

Прокси-сервер KSN (точки распространения)

В разделе **Прокси-сервер KSN (точки распространения)** вы можете настроить приложение так, чтобы точка распространения использовалась для пересылки KSN запросов от управляемых устройств.

- **Включить прокси-сервер KSN на стороне точки распространения**

  Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

  Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского".

  По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены в окне свойств Сервера администрирования.

  Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

- **Порт**

  Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

- **UDP-порт**

  Чтобы Агент администрирования подключался к Серверу администрирования через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **Номер UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к Серверу администрирования выполняется через UDP-порт 15000.

История ревизий

На вкладке **История ревизий** вы можете:

- Просмотреть и сохранить историю изменений политики.
- Откатить к ревизии политики.
- Добавить и изменить описание ревизии политики.
- Сравнить ревизии политики.

Сравнение параметров политики Агента администрирования по операционным системам

В таблице ниже показано, какие параметры политики Агента администрирования можно использовать для настройки Агента администрирования для конкретной операционной системы.

Параметры политики Агента администрирования: сравнение по операционным системам

Раздел Политики	Windows	macOS	Linux
Общие	✓	✓	✓
Настройка событий	✓	✓	✓
Параметры	✓	✓ Кроме флажка **Использовать пароль деинсталляции**.	✓ Кроме флажка **Использовать пароль деинсталляции**.
Хранилища	✓	✓ Функциональность **Информация о реестре оборудования** доступна.	✓ Доступна функциональность: • **Информация об установленных приложениях** • **Информация о реестре оборудования**
Обновления и уязвимости в приложениях	✓	—	—
Управление перезагрузкой	✓	—	—
Совместный доступ к рабочему столу Windows	✓	—	—
Управление патчами и обновлениями	✓	—	—
Подключения → Сеть	✓	✓ Кроме флажка **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**.	✓ Кроме флажка **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**.
Подключения → Расписание соединений	✓	✓	✓
Опрос сети точками распространения	✓ Доступны следующие параметры: • **Сеть Windows** • **IP-диапазоны** • **Контроллеры доменов** (Microsoft Active Directory)	—	✓ Доступны следующие параметры: • **IP-диапазоны** • **Контроллеры доменов** (Microsoft Active Directory, Samba как Active Directory)
Параметры сети для точек распространения	✓	✓	✓
Прокси-сервер KSN (точки распространения)	✓	—	✓

Настройка параметров защиты управляемых приложений

Для настройки параметров защиты управляемых приложений "Лаборатории Касперского" вы можете использовать политики.

Подробнее о настройке политик Kaspersky Endpoint Security см. в соответствующей справке:

- Справка Kaspersky Endpoint Security для Windows
- Справка Kaspersky Endpoint Security для Linux
- Справка Kaspersky Endpoint Security для Mac

Ручная настройка групповой задачи обновления Kaspersky Endpoint Security

Оптимальный и рекомендуемый вариант расписания для Kaspersky Endpoint Security **При загрузке обновлений в хранилище** при установленном флажке **Использовать автоматическое определение случайного интервала между запусками задачи**.

Управление задачами

В этом разделе описаны задачи, которые используются в Open Single Management Platform.

О задачах

Open Single Management Platform управляет работой приложений безопасности "Лаборатории Касперского", установленных на устройствах, путем создания и запуска задач. С помощью *задач* выполняются установка, запуск и остановка приложений, проверка файлов, обновление баз и модулей приложений, другие действия с приложениями. Задачи могут выполняться на Сервере администрирования и на устройствах.

На устройствах выполняются следующие типы задач:

- *Локальные задачи* – это задачи, которые выполняются на конкретном устройстве.

  Локальные задачи может изменять не только администратор средствами администрирования, но и пользователь удаленного устройства (например, в интерфейсе приложения безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

- *Групповые задачи* – это задачи, которые выполняются на всех устройствах указанной группы.

  Если иное не указано в свойствах задачи, групповая задача также распространяется на подгруппы указанной группы.

- *Глобальные задачи* – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.

Для каждого приложения вы можете создавать несколько групповых задач, задач для наборов устройств и локальных задач.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущено приложение, для которого созданы эти задачи.

Результаты выполнения задач сохраняются в журнале событий операционной системы на каждом устройстве и в базе данных Сервера администрирования.

Не используйте в параметрах задач конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

Область задачи

Область применения задачи – это подмножество устройств, на которых выполняется задача. Существуют следующие типы областей задачи:

- Область *локальной задачи* – само устройство.
- Область *задачи Сервера администрирования* – Сервер администрирования.
- Область *групповой задачи* – перечень устройств, входящих в группу.

При создании *глобальной задачи* можно использовать следующие методы определения ее области:

- Вручную указать требуемые устройства.

  В качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал) или DNS-имя. Также можно выбрать устройства, обнаруженные в сети Сервером администрирования.

- Импортировать список устройств из файла формата TXT, содержащего перечень адресов добавляемых устройств (каждый адрес должен располагаться в отдельной строке).

  Если список устройств импортируется из файла или формируется вручную, а устройства идентифицируются по имени, то в список могут быть добавлены только те устройства, информация о которых уже занесена в базу данных Сервера администрирования. Данные должны быть занесены в базу при подключении этих устройств или в результате обнаружения устройств.

- Указать выборку устройств.

  С течением времени область действия задачи изменяется по мере того, как изменяется множество устройств, входящих в выборку. Выборка устройств может быть построена на основе атрибутов устройств, в том числе на основе установленного на устройстве программного обеспечения, а также на основе присвоенных устройству тегов. Выборка устройств является наиболее гибким способом задания области действия задачи.

  Запуск по расписанию задач для выборок устройств всегда осуществляет Сервер администрирования. Такие задачи не запустятся на устройствах, не имеющих связи с Сервером администрирования. Задачи, область действия которых задается другим способом, запускаются непосредственно на устройствах и не зависят от наличия связи устройства с Сервером администрирования.

  Задачи для выборок устройств будут запускаться не по локальному времени устройства, а по локальному времени Сервера администрирования. Задачи, область действия которых задается другим способом, запускаются по локальному времени устройства.

Создание задачи

Вы можете создать задачу в списке задач. Также можно выбрать устройства в списке **Управляемые устройства** и создать задачу, назначенную выбранным устройствам.

Чтобы создать задачу в списке задач:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте шагам мастера.
3. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
4. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.

Чтобы создать задачу, назначенную выбранным устройствам:

В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства**.

Отобразится список управляемых устройств.

1. В списке управляемых устройств установите флажки рядом с устройствами, для которых нужно запустить задачу. Вы можете использовать функции поиска и фильтрации, чтобы найти необходимые устройства.
2. Нажмите на кнопку **Запустить задачу** и выберите **Создать задачу**.

   Запустится мастер создания задачи.

   На первом шаге мастера вы можете удалить устройства, выбранные для включения в область применения задачи. Следуйте инструкциям мастера.
3. Нажмите на кнопку **Готово**.

Задача создана для выбранных устройств.

Просмотр списка задач

Вы можете просмотреть список задач, созданных в Kaspersky SIEM Cloud.

Чтобы просмотреть список задач,

в главном окне приложения перейдите в раздел **Задачи**.

Отобразится список задач. Задачи сгруппированы по названиям приложений, к которыми они относятся. Например, задача *Удаленная деинсталляция приложения* относится к Серверу администрирования, а задача *Поиск уязвимостей и требуемых обновлений* относится к Агенту администрирования.

Чтобы просмотреть свойства задачи,

нажмите на имя задачи.

Окно свойств задачи отображается с несколькими именными вкладками. Например, **Тип задачи** отображается на вкладке **Общие**, а расписание задачи на вкладке **Расписание**.

Запуск задачи вручную

Приложение запускает задачи в соответствии с расписанием, заданным в свойствах каждой задачи. Вы можете запустить задачу вручную в любое время из списка задач. Также можно выбрать устройства в списке **Управляемые устройства** и запустить для них существующую задачу.

Чтобы запустить задачу вручную:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. В отобразившемся списке задач установите флажок напротив задачи, которую вы хотите запустить.
3. Нажмите на кнопку **Запустить**.

Задача будет запущена. Вы можете проверить статус задачи в столбце **Статус** или нажав на кнопку **Результат выполнения**.

Запуск задачи для выбранных устройств.

Вы можете выбрать одно или несколько клиентских устройств в списке устройств, а затем запустить для них ранее созданную задачу. Это позволяет запускать задачи, созданные ранее для заданного набора устройств.

Это действие изменит в задаче список устройств, к которым применяется эта задача.

Чтобы запустить задачу для выбранных устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**. Отобразится список управляемых устройств.
2. В списке управляемых устройств с помощью флажков выберите устройства, для которых будет выполняться задача. Вы можете использовать функции поиска и фильтрации, чтобы найти необходимые устройства.
3. Нажмите на кнопку **Запустить задачу** и выберите **Использовать существующую задачу**.

   Отобразится список существующих задач.
4. Выбранные устройства отображаются над списком задач. При необходимости вы можете удалить устройство из этого списка. Вы можете удалить все устройства, кроме одного.
5. Выберите необходимую задачу в списке. Вы можете использовать поле поиска над списком для поиска задачи по ее названию. Можно выбрать только одну задачу.

6. Сохраните изменения, нажав на одну из кнопок:

- **Запустить и закрыть**

  Задача запускается для выбранных устройств.

- **Запустить и открыть задачу**

Задача запускается для выбранных устройств и отображается окно свойств задачи, где вы можете быстро просмотреть результаты ее выполнения.

Параметры запуска по расписанию в задаче не меняются.

Общие параметры и свойства задач

Этот раздел содержит описание параметров, которые вы можете просмотреть и настроить для большинства ваших задач. Список доступных параметров зависит от настраиваемой задачи.

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- Окно Выбор устройств, которым будет назначена задача:

  - **Назначить задачу группе администрирования**

    Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

    Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

    Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, так как групповые задачи подчиняются параметрам групп безопасности, к которым они относятся.

  - **Задать адреса устройств вручную или импортировать из списка**

    В этом случае задача назначается набору устройств. Можно указать устройство одним из следующих способов:

    - Укажите IP-адрес, NetBIOS-имя или DNS-имя устройства.

    - Укажите IP-диапазон.

      Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

    - Выберите устройства, обнаруженные Сервером администрирования, включая нераспределенные устройства.

      Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

- **Назначить задачу выборке устройств**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

- Параметры учетной записи:

  - **Учетная запись по умолчанию**

    Задача будет запускаться под той же учетной записью, под которой было установлено и запущено приложение, выполняющее эту задачу.

    По умолчанию выбран этот вариант.

  - **Задать учетную запись**

    В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

- Параметры перезагрузки операционной системы:

  - **Не перезагружать**

    Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

  - **Перезагрузить устройство**

    В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

  - **Запрашивать у пользователя**

    На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

    По умолчанию выбран этот вариант.

  - **Повторять запрос каждые (мин)**

    Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

    По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

    Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

  После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать приложения в заблокированных сеансах**

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

Параметры, заданные после создания задачи

Вы можете задать следующие параметры только после создания задачи.

- Параметры групповой задачи:

  - **Распространить на подгруппы**

    Этот параметр доступен только в свойствах групповых задач.

    Когда этот параметр включен, область действия задачи включает в себя:

    - группу администрирования, которую вы выбрали при создании задачи;
    - группы администрирования, подчиненные по отношению к выбранной группе администрирования на любом уровне вниз по иерархии групп.

    Если этот параметр выключен, в состав задачи входит только та группа администрирования, которую выбрали при создании задачи.

    По умолчанию параметр включен.

  - **Распространить на подчиненные и виртуальные Серверы администрирования**

    При включении этого параметра задача, действующая на главном Сервере администрирования, применяется и на подчиненных Серверах администрирования (в том числе виртуальных). Если на подчиненном Сервере администрирования уже существует задача такого же типа, то на подчиненном Сервере администрирования применяются обе задачи – существующая и унаследованная от главного Сервера администрирования.

    Этот параметр доступен, только если параметр **Распространить на подгруппы** включен.

    По умолчанию параметр выключен.

- Параметры расписания задачи:

Типы расписаний могут изменяться в зависимости от задачи.

- **Параметры Запуск задачи:**
  - **Вручную**

    Задача не запускается автоматически. Вы можете запустить задачу только вручную.

    По умолчанию выбран этот вариант.

  - **Один раз**

    Задача выполняется один раз, в указанные дату и время (по умолчанию в день создания задачи).

  - **Немедленно**

    Задача запускается сразу после сохранения ее параметров.

  - **Каждые N минут**

    Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

    По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

  - **Каждый N час**

    Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

    По умолчанию задача запускается каждые 6 часов, начиная с текущих системной даты и времени.

  - **Каждые N дней**

    Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются приложением, для которого вы создаете задачу.

    По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

  - **По дням недели**

    Задача выполняется регулярно, в указанные дни недели, в указанное время.

    По умолчанию задача запускается каждую пятницу в 18:00:00.

  - **Ежемесячно**

    Задача выполняется регулярно, в указанный день месяца, в указанное время.

    В месяцах, у которых нет указанного дня, задача выполняется в последний день.

    По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

  - **Ежемесячно в выбранный день**

    Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

По умолчанию указано время 18:00 и не выбраны дни месяца.

> Обратите внимание, что вы выбираете порядковый номер дня недели в месяце, а не конкретную дату в месяце или номер недели (первая, вторая неделя месяца). Например, если вы выберите ячейку **Вт** в строке **Первая**, в этом случае задача будет запускаться каждый первый вторник каждого нового месяца.

Вы можете выбрать несколько дней недели.

- **При загрузке обновлений в хранилище**

  Эта задача запускается после загрузки обновлений в хранилище. Например, вам может понадобиться это расписание для задачи *Обновление*.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы приложений, которые будут отслеживать вирусные атаки. Доступны следующие типы приложений:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы приложений.

  Вы можете запускать разные задачи в зависимости от типа приложения безопасности, сообщающего о вирусной атаке. В этом случае удалите выбор типов приложений, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам. Например, вы можете запустить задачу *Управление устройствами* с помощью параметра **Включить устройство** и после ее завершения запустить задачу *Поиск вирусов*, как запускающую задачу.

  Вам нужно выбрать запускающую задачу из таблицы и статус, с которым эта задача должна завершиться (**Завершена успешно** или **Сбой**).

  При необходимости вы можете искать, сортировать и фильтровать задачи в таблице следующим образом:

  - Введите название задачи в поле поиска, чтобы выполнить поиск задачи по названию.
  - Нажмите на значок сортировки, чтобы отсортировать задачи по имени.

    По умолчанию задачи отсортированы в алфавитном порядке по возрастанию.
  - Нажмите на значок фильтра и в открывшемся окне отфильтруйте задачи по группам, после чего нажмите на кнопку **Применить**.

Параметры расписания могут **зависеть от местного часового пояса операционной системы устройства**.

Корреляция между локальным часовым поясом операционной системы устройства и временем запуска задачи

Расписание задачи	Используется местное время
Один раз	Нет
Каждые N минут	Нет
Каждый N час	Нет
Каждые N дней	Да
По дням недели	Да
Ежемесячно	Да
Ежемесячно в выбранный день	Да
При загрузке обновлений в хранилище	Другое условие для запуска задачи (соответствует названию расписания)
При обнаружении вирусной атаки	Другое условие для запуска задачи (соответствует названию расписания)
По завершении другой задачи	Другое условие для запуска задачи (соответствует названию расписания)
Немедленно	Другое условие для запуска задачи (соответствует названию расписания)
Вручную	Другое условие для запуска задачи (соответствует названию расписания)

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию. Для расписания **Вручную**, **Один раз** и **Немедленно** задачи выполняются только на тех клиентских устройствах, которые видны в сети. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр включен.

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

- **Включать устройства перед запуском задачи функцией Wake-on-LAN**

  Если флажок установлен, операционная система на устройстве будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут.

  Включите этот параметр, если вы хотите, чтобы задача выполнялась на всех клиентских устройствах из области задач, включая те устройства, которые выключены, когда задача вот-вот начнется.

  Если нужно, чтобы устройства автоматически выключались после выполнения задачи, включите параметр **Выключать устройства после выполнения задачи**. Параметр находится в этом же окне.

  По умолчанию параметр выключен.

- **Выключать устройства после выполнения задачи**

  Например, вы можете включить этот параметр для задачи установки обновлений, которая устанавливает обновления на клиентские устройства каждую пятницу после рабочего времени, а затем выключает эти устройства на выходные.

  По умолчанию параметр выключен.

- **Остановить, если задача выполняется дольше**

  По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

  Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

  По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

- Уведомления:

  - Блок **Сохранять информацию о результатах**:

    - **Сохранять все события**

    - **Сохранять события, связанные с ходом выполнения задачи**

    - **Сохранять только результат выполнения задачи**

    - **Хранить в базе данных Сервера администрирования в течение (сут)**

      События приложения, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся на Сервере администрирования в течение указанного количества дней. По истечении этого периода информация удаляется с Сервера администрирования.

      По умолчанию параметр включен.

    - **Хранить в журнале событий ОС на устройстве**

      События приложения, связанные с выполнением задачи, хранятся локально в системном журнале событий каждого клиентского устройства.

      По умолчанию параметр выключен.

  - **Уведомлять только об ошибках**

  - **Уведомлять по электронной почте**

- Параметры области действия задачи
- **Исключения из области**

  Вы можете указать группу устройств, к которым не применяется задача. Группы, подлежащие исключению, могут быть только подгруппами группы администрирования, к которой применяется задача.
- **История ревизий**

Экспорт задачи

Open Single Management Platform позволяет сохранить задачу и ее параметры в файл KLT. Вы можете использовать файл KLT для импорта сохраненной задачи как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

Чтобы экспортировать задачу:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Установите флажок рядом с задачей, которую вы хотите экспортировать.

   Невозможно экспортировать несколько задач одновременно. Если вы выберете несколько задач, кнопка **Экспортировать** будет неактивна. Задачи Сервера администрирования также недоступны для экспорта.
3. Нажмите на кнопку **Экспортировать**.
4. В открывшемся окне **Сохранить как** укажите имя файла задачи и путь. Нажмите на кнопку **Сохранить**.

   Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл задачи автоматически сохраняется в папку **Загрузки**.

Импорт задачи

Open Single Management Platform позволяет импортировать задачу из файла KLT. Файл KLT содержит экспортированную задачу и ее параметры.

Для корректного импорта задачи приложения "Лаборатории Касперского" нужно установить соответствующий плагин управления.

Чтобы импортировать задачу:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Импортировать**.
3. Нажмите на кнопку **Обзор**, чтобы выбрать файл задачи, которую вы хотите импортировать.
4. В открывшемся окне укажите путь к файлу KLT задачи и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл задачи.

   Начнется обработка задачи.

5. После того как задача будет успешно обработана, выберите устройства, которым вы хотите назначить задачу. Для этого выберите один из следующих параметров:

   - **Назначить задачу группе администрирования**

     Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

     Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

     Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, так как групповые задачи подчиняются параметрам групп безопасности, к которым они относятся.

   - **Задать адреса устройств вручную или импортировать из списка**

     Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

     Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

   - **Назначить задачу выборке устройств**

     Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

     Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

6. Укажите область действия задачи.

7. Нажмите на кнопку **Завершить**, чтобы завершить задачу импорта.

Появится уведомление с результатами импорта. Если задача успешно импортирована, вы можете перейти по ссылке **Подробнее** для просмотра свойств задачи.

После успешного импорта задача отображается в списке задач. Параметры задачи и расписание также импортируются. Задача будет запущена в соответствии с расписанием.

Если имя новой импортированной задачи идентично имени существующей задачи, имя импортированной задачи расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Просмотр результатов выполнения задач, хранящихся на Сервере администрирования

Kaspersky SIEM Cloud позволяет просматривать результаты выполнения групповых задач, задач для наборов устройств и задач Сервера администрирования.

Чтобы посмотреть результаты выполнения задачи:

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.

Управление клиентскими устройствами

Kaspersky SIEM Cloud позволяет управлять клиентскими устройствами:

- Просматривать параметры и статусы управляемых устройств, в том числе кластеров и массивов серверов.
- Настраивать точки распространения.
- Управлять задачами.

Группы администрирования можно использовать для объединения клиентских устройств в набор, которым можно управлять как единым целым. Клиентское устройство может быть включено только в одну группу администрирования. Устройства могут быть автоматически отнесены к группе на основе **Условия правила:**

- Создание правил перемещения устройств.
- Копирование правил перемещения устройств.
- Условия для правила перемещения устройств.

Вы можете использовать выборки устройств, чтобы для фильтровать устройства по условию. Вы также можете назначать теги устройствам для создания выборок устройств, поиска устройств и распределения устройств между группами администрирования.

Параметры управляемого устройства

Чтобы просмотреть параметры управляемого устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием нужного устройства.

Откроется окно свойств выбранного устройства.

В верхней части окна свойств отображаются следующие вкладки, на которых представлены основные группы параметров:

- **Общие**

  Эта вкладка содержит следующие разделы:

  - Раздел **Общие** содержит общую информацию о клиентском устройстве. Информация предоставляется на основании данных, полученных в ходе последней синхронизации клиентского устройства с Сервером администрирования:

    - **Имя**

      В поле можно просмотреть и изменить имя клиентского устройства в группе администрирования.

    - **Описание**

      В поле можно ввести дополнительное описание клиентского устройства.

    - **Статус устройства**

      Статус клиентского устройства, формируемый на основании установленных администратором критериев состояния антивирусной защиты на устройстве и активности устройства в сети.

    - **Владелец устройства**

      Имя владельца устройства. Вы можете назначить или удалить пользователя в качестве владельца устройства, нажав на ссылку **Сменить владельца устройства**.

    - **Полное название группы**

      Группа администрирования, в состав которой входит клиентское устройство.

    - **Последнее обновление антивирусных баз**

      Дата последнего обновления антивирусных баз или приложений на устройстве.

    - **Соединение с Сервером администрирования**

      Дата и время последнего соединения Агента администрирования, установленного на клиентском устройстве, с Сервером администрирования.

    - **Последнее появление в сети**

      Дата и время, когда устройство в последний раз было видимо в сети.

    - **Версия Агента администрирования**

      Версия установленного Агента администрирования.

    - **Создано**

      Дата создания устройства в Open Single Management Platform.

- **Синхронизировать сейчас**

  Несмотря на то что Open Single Management Platform автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, в отдельных случаях администратору нужно точно знать, что в текущий момент для определенного устройства синхронизация выполнена.

  Если вы нажмете на кнопку **Синхронизировать сейчас**, приложение синхронизирует выбранное устройство с Сервером администрирования.

- **Не разрывать соединение с Сервером администрирования**

  Если этот параметр включен, сохраняется постоянное соединение между управляемым устройством и Сервером администрирования. Вы можете использовать этот параметр, если не используете push-серверы, которые обеспечивают такое соединение.

  Если параметр выключен и push-серверы не используются, управляемое устройство подключается к Серверу администрирования для синхронизации данных или передачи информации.

  Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

  Этот параметр по умолчанию выключен на управляемых устройствах. Этот параметр включен по умолчанию на устройстве, на котором установлен Сервер администрирования, и остается включенным, даже если вы попытаетесь его выключить.

- **Сеансы**

  В этом разделе содержится таблица с информацией о пользователях, которые в настоящее время выполнили вход на устройство. В таблице отображаются следующие данные в соответствующих столбцах:

  - Имя пользователя.
  - SAM-имя.
  - Имя участника.
  - Адрес электронной почты.

  Для корректного отображения информации о сеансах доменных пользователей, вам нужно использовать опрос контроллера домена.

- В разделе **Сеть** отображается следующая информация о сетевых свойствах клиентского устройства:

  - **IP-адрес**

    IP-адрес устройства

  - **Windows-домен**

    Рабочая группа, содержащая устройство.

  - **DNS-имя**

    Имя DNS-домена клиентского устройства.

  - **NetBIOS-имя**

    NetBIOS-имя клиентского устройства.

- **IPv6-адрес**

  IPv6-адрес клиентского устройства.

- В разделе **Система** представлена информация об операционной системе, установленной на клиентском устройстве:

  - **ОС**
  - **Архитектура процессора**
  - **Имя устройства**
  - **Тип виртуальной машины**

    Производитель виртуальной машины

  - **Динамическая виртуальная машина как часть VDI**

    В этой строке показано, является ли клиентское устройство динамической виртуальной машиной как часть VDI.

  - **Сборка ОС**

- В разделе **Защита** представлена следующая информация о состоянии антивирусной защиты на клиентском устройстве:

  - **Видимо в сети**

    Статус видимости клиентского устройства.

  - **Статус устройства**

    Статус клиентского устройства, формируемый на основании установленных администратором критериев состояния антивирусной защиты на устройстве и активности устройства в сети.

  - **Описание статуса**

    Статус защиты клиентского устройства и подключения к Серверу администрирования.

  - **Состояние защиты**

    Статус текущего состояния постоянной защиты клиентского устройства.

    После того как статус изменяется на устройстве, новый статус отображается в окне свойств устройства только после синхронизации клиентского устройства с Сервером администрирования.

  - **Последняя полная проверка**

    Дата и время последнего поиска вредоносного ПО на клиентском устройстве.

  - **Обнаружен вирус**

    Общее количество обнаруженных на клиентском устройстве угроз с момента установки приложения безопасности (первой проверки устройства) либо с момента последнего обнуления счетчика угроз.

- **Объекты, которые не удалось вылечить**

  Количество необработанных файлов на клиентском устройстве.

  В поле не учитывается количество необработанных файлов для мобильных устройств.

- **Статус шифрования дисков**

  Текущее состояние шифрования файлов на локальных дисках устройства. Описание статусов см. в онлайн-справке Kaspersky Endpoint Security for Windows.

  Файлы могут быть зашифрованы только на управляемых устройствах, на которых установлен Kaspersky Endpoint Security for Windows.

- **Просмотреть ошибки шифрования данных**

  Информация об ошибках шифрования данных на устройствах. Шифрование выполняется функцией Шифрование данных приложений "Лаборатории Касперского". Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования.

- В разделе **Статус устройства определен приложением** отображается информация о статусе устройства, который определен управляемым приложением, установленным на клиентском устройстве. Это состояние устройства может отличаться от того, которое определено Kaspersky SIEM Cloud.

- **Приложения**

  На этой вкладке отображается список приложений "Лаборатории Касперского", установленных на клиентском устройстве. На этой вкладке находятся кнопки **Запустить** и **Остановить**, которые позволяют запускать и останавливать выбранное приложение "Лаборатории Касперского" (кроме Агента администрирования). Вы можете использовать эти кнопки, если на управляемых устройствах доступен порт 15000 UDP для приема запросов на связь с Сервером администрирования. Если управляемое устройство недоступно для push-уведомлений, но включен режим постоянного подключения к Серверу администрирования (параметр **Не разрывать соединение с Сервером администрирования** в разделе **Общие** включен), кнопки **Запустить** и **Остановить** активны. Иначе при попытке запустить или остановить приложение появится сообщение об ошибке. Также вы можете нажать на имя приложения, чтобы просмотреть общую информацию о приложении, список событий, произошедших на устройстве, и параметры приложения.

- **Действующие политики и профили политик**

  На этой вкладке отображаются списки политик и профилей политик, которые назначены управляемому устройству.

- **Задачи**

  На вкладке **Задачи** вы можете управлять задачами клиентского устройства: просматривать список существующих задач, создавать новые, удалять, запускать и останавливать задачи, изменять их параметры и просматривать результаты выполнения. Список задач предоставляется на основании данных, полученных в ходе последней синхронизации клиента с Сервером администрирования. Информация о статусе задач запрашивается Сервером администрирования с клиентского устройства. Если на управляемых устройствах доступен порт 15000 UDP для приема запросов на связь с Сервером администрирования, отображается статус задачи и кнопки управления задачей активны. Если push-сервер не может получить доступ к управляемому устройству, но включен режим постоянного подключения к Серверу администрирования (параметр **Не разрывать соединение с Сервером администрирования** с Сервером администрирования в разделе **Общие** включен), действия с задачами доступны.

  В случае отсутствия связи статус не отображается и кнопки неактивны.

- **События**

  На вкладке **События** отображаются события, зарегистрированные на Сервере администрирования для выбранного клиентского устройства.

  Вы можете экспортировать, копировать и удалять события устройства.

- **Проблемы безопасности**

  На вкладке **Проблемы безопасности** можно просматривать, изменять и создавать проблемы безопасности для клиентского устройства. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором. Например, если пользователь постоянно переносит на устройство вредоносные приложения с личного съемного диска, администратор может создать проблему безопасности. Администратор может указать краткое описание случая и рекомендуемых действий (таких как дисциплинарные действия), которые должны быть предприняты против пользователя в тексте проблемы безопасности, и может добавить ссылку на пользователя или пользователей.

  Проблема безопасности, для которой выполнены необходимые действия, называется *обработанным*. Наличие необработанных проблем безопасности может быть выбрано условием для изменения статуса устройства на *Критический* или *Предупреждение*.

  В разделе содержится список проблем безопасности, созданных для устройства. Проблемы безопасности классифицируются по уровню важности и типу. Тип проблемы безопасности определяется приложением "Лаборатории Касперского", которое создает проблему безопасности. Обработанные проблемы безопасности можно отметить в списке, установив флажок в столбце **Обработана**.

- **Теги**

  На вкладке **Теги** можно управлять списком ключевых слов, на основании которых выполняется поиск клиентского устройства: просматривать список существующих тегов, назначать теги из списка, настраивать правила автоматического назначения тегов, добавлять новые теги и переименовывать старые теги, удалять теги.

- **Дополнительно**

  Эта вкладка содержит следующие разделы:

  - **Реестр приложений**. В этом разделе можно просмотреть реестр установленных на клиентском устройстве приложений и обновлений для них, а также настроить отображение реестра приложений.

    Информация об установленных приложениях предоставляется в том случае, если установленный на клиентском устройстве Агент администрирования передает необходимую информацию на Сервер администрирования. Параметры передачи информации на Сервер администрирования можно настроить в окне свойств Агента администрирования или его политики в разделе **Хранилища**.

    При нажатии на имя приложения открывается окно, содержащее сведения о приложении и список пакетов обновлений, установленных для этого приложения.

  - **Исполняемые файлы**. В этом разделе отображаются исполняемые файлы, обнаруженные на клиентском устройстве.

  - **Точки распространения**. В этом разделе представлен список точек распространения, с которыми взаимодействует устройство.

    - **Экспортировать в файл**

      По кнопке **Экспортировать в файл** вы можете сохранить в файл список точек распространения, с которыми взаимодействует устройство. По умолчанию приложение экспортирует список устройств в файл формата CSV.

- **Свойства**

  По кнопке **Свойства** вы можете посмотреть и настроить параметры точки распространения, с которым взаимодействует устройство.

- **Реестр оборудования**. В этом разделе можно просмотреть информацию об оборудовании, установленном на клиентском устройстве.

  Если Агент администрирования установлен на устройстве с операционной системой Windows, он отправляет на Сервер администрирования следующую информацию об аппаратном обеспечении устройства:

  - оперативная память;
  - запоминающие устройства;
  - материнская плата;
  - процессор;
  - сетевой адаптер;
  - мониторы;
  - видеоадаптер;
  - звуковая плата.

  Если Агент администрирования установлен на устройстве с операционной системой Linux или macOS, он отправляет на Сервер администрирования следующую информацию об аппаратном обеспечении устройства, если эта информация предоставляется операционной системой:

  - общий объем оперативной памяти;
  - общий объем запоминающих устройств;
  - материнская плата;
  - процессор;
  - сетевой адаптер.

- **Применимые обновления**. В этом разделе можно просмотреть список обнаруженных на устройстве обновлений программного обеспечения, которые не были установлены.

- **Уязвимости в приложениях**. В этом разделе можно просмотреть список с информацией об уязвимостях сторонних приложений, установленных на клиентских устройствах.

  Чтобы сохранить уязвимости в файл, установите флажки рядом с уязвимостями, которые вы хотите сохранить, и нажмите на кнопку **Экспортировать в CSV** или на кнопку **Экспортировать в TXT**.

  Раздел содержит следующие параметры:

  - **Показывать только те уязвимости, которые можно закрыть**

    Если параметр включен, в разделе отображаются уязвимости, которые можно закрыть патчем.

    Если параметр выключен, в разделе отображаются и уязвимости, которые можно закрыть патчем, и уязвимости, для которых патч отсутствует.

По умолчанию параметр включен.

- **Свойства уязвимости**

  Нажмите на имя уязвимости в приложениях в списке, чтобы просмотреть свойства выбранной уязвимости в приложениях в отдельном окне. В окне свойств можно выполнить следующие действия:

  - Пропустить уязвимость в приложениях на этом управляемом устройстве (в OSMP Console).
  - Просмотреть список рекомендуемых исправлений для уязвимости.
  - Вручную указать обновления программного обеспечения для закрытия уязвимости (в OSMP Console).
  - Просмотреть экземпляр уязвимости.
  - Просмотреть список существующих задач для закрытия уязвимости и создать задачи для закрытия уязвимости.

- **Удаленная диагностика**. В этом разделе можно выполнять удаленную диагностику клиентских устройств.

Проверка соединения клиентского устройства с Сервером администрирования вручную Утилита klnagchk

Вы можете проверять соединение и получать подробную информацию о параметрах подключения клиентского устройства к Серверу администрирования с помощью утилиты klnagchk. Утилита klnagchk находится в папке установки Агента администрирования.

При запуске из командной строки утилита klnagchk в зависимости от используемых ключей выполняет следующие действия:

- Выводит на экран или заносит в файл журнала событий значения параметров подключения Агента администрирования, установленного на устройстве, к Серверу администрирования.
- Записывает в файл журнала событий статистику Агента администрирования (с момента его последнего запуска) и результаты выполнения утилиты либо выводит информацию на экран.
- Пытается установить соединение Агента администрирования с Сервером администрирования.

  Если соединение установить не удалось, утилита посылает ICMP-пакет для проверки статуса устройства, на котором установлен Сервер администрирования.

Чтобы проверить соединение клиентского устройства с Сервером администрирования с помощью утилиты klnagchk,

на устройстве с установленным Агентом администрирования запустите утилиту klnagchk из командной строки под учетной записью локального администратора.

Синтаксис командной строки утилиты:

```
klnagchk [-logfile <file name>] [-sp] [-savecert <path to the certificate file>] [-
restart][-sendhb]
```

Описания ключей:

- `-logfile <file name>` – записывает значения параметров подключения Агента администрирования к Серверу и результаты выполнения утилиты в файл журнала.

  По умолчанию информация сохраняется в стандартном потоке вывода (stdout). Если ключ не используется, параметры, результаты и сообщения об ошибках выводятся на экран.

- `-sp` – выводит пароль для аутентификации пользователя на прокси-сервере.

  Ключ используется, если подключение к Серверу администрирования осуществляется через прокси-сервер.

- `-savecert <file name>` – сохраняет сертификат для аутентификации доступа к Серверу администрирования в указанном файле.

- `-restart` – запускает Агент администрирования после завершения работы утилиты.

- `-sendhb` – запускает синхронизацию Агента администрирования с Сервером администрирования.

После запуска утилита klnagchk обращается к конфигурационным файлам Агента администрирования и отображает параметры подключения. Эти параметры задаются при установке Агента администрирования и в параметрах политики Агента администрирования:

- `Current device` – имя клиентского устройства в сети Windows.

- `Network Agent version` – номер версии Агента администрирования (с патчами), установленного на устройстве.

- `Server address` – адрес Сервера администрирования.

- `Use SSL` – параметр, указывающий, используется ли защищенное соединение при подключении к Серверу администрирования.

  Возможные значения:

  - 0 – защищенный канал не используется.

  - 1 – используется защищенный канал.

- `Compress traffic` – параметр, указывающий, сжимается ли трафик между клиентским устройством и Сервером администрирования.

- `Server SSL ports` – номера допустимых портов для подключения к Серверу администрирования при использовании защищенного канала.

- `Server ports` – номера портов, допустимых для подключения к Серверу администрирования при использовании обычного соединения.

- `Use proxy server` – параметр, указывающий, используется ли прокси-сервер.

  Возможные значения:

  - 0 – прокси-сервер не используется.

  - 1 – прокси-сервер используется.

- `Address` – адрес и порт прокси-сервера, разделенные двоеточием. Этот параметр отображается, только если используется прокси-сервер.

- `User name` – имя пользователя для доступа к прокси-серверу. Этот параметр отображается, только если используется прокси-сервер.

- `Password` – пароль для доступа к прокси-серверу. Этот параметр отображается, только если используется прокси-сервер. Чтобы показать пароль прокси-сервера, вам нужно использовать в команде ключ `sp`.

- `Certificate` – параметр, указывающий, есть ли у клиентского устройства сертификат Сервера администрирования. Сертификат может не существовать, например, если Агент администрирования ни разу не подключился к Серверу администрирования.

  Возможные значения:

  - `not installed` – на клиентском устройстве отсутствует сертификат Сервера администрирования.

  - `present` – клиентское устройство имеет сертификат Сервера администрирования.

- `Open UDP port` – параметр, указывающий, использует ли Агент администрирования UDP-порт для получения запросов на синхронизацию от Сервера администрирования.

  Возможные значения:

  - 0 – UDP-порт закрыт для приема запросов на синхронизацию от Сервера администрирования.

  - 1 – UDP-порт открыт для приема запросов на синхронизацию от Сервера администрирования.

- `UDP ports` – номера UDP-портов, которые может использовать Агент администрирования.

- `Location name` – сетевое местоположение устройства.

- `State of network location` – параметр, указывающий, можно ли переключить клиентское устройство с одного профиля соединений Сервера администрирования на другой.

  Возможные значения:

  - `Enabled` – профиль соединений к Серверу администрирования можно переключить для клиентского устройства.

  - `Disabled` – профиль соединений к Серверу администрирования переключить для клиентского устройства невозможно.

- `Profile to use` – профиль соединений к Серверу администрирования.

- `Condition` – IP-адрес и маска подсети сети, к которой подключено клиентское устройство.

- `Ping period, minutes` – стандартный интервал синхронизации.

- `Conn timeout, s` – время ожидания соединения.

- `RW timeout, s` – время ожидания соединения для операций чтения-записи.

- `Host ID` – идентификатор устройства в сети. `Device ID` уникален для клиентских устройств, управляемых определенным Сервером администрирования.

- `Locations of connection gateways` – параметры подключения клиентского устройства к Серверу администрирования с помощью шлюза соединения.

- `Location of distribution points` – параметры подключения клиентского устройства к Серверу администрирования с помощью точки распространения.

- `Connection with server` – параметр, указывающий, имеет ли шлюз соединения постоянное соединение с Сервером администрирования. Параметр отображается только в том случае, если клиентское устройство выступает в роли шлюза соединения.

  Возможные значения:

  - `active` – шлюз соединения имеет постоянное соединение с Сервером администрирования.

  - `inactive` – шлюз соединения не имеет постоянного соединения с Сервером администрирования.

- `Connection with server through connection gateway` – параметр, указывающий, правильно ли установлено соединение с Сервером администрирования с помощью шлюза соединения. Параметр отображается только в том случае, если клиентское устройство выступает в роли шлюза соединения.

  Возможные значения:

  - `active` – соединение с Сервером администрирования с помощью шлюза соединения установлено правильно.

  - `inactive` – соединение с Сервером администрирования с помощью шлюза соединения установлено некорректно.

Также вывод утилиты klnagchk может содержать одну из следующих строк:

- `Administration Server is installed on this device` – на устройстве Сервера администрирования запущена утилита klnagchk.

- `This device has been assigned a connection gateway but is not yet registered on Administration Server` – утилита klnagchk запущена на устройстве, на котором установлен Агент администрирования, выполняющий роль шлюза соединения. Настроенный шлюз соединения ожидает соединения от Сервера администрирования, но Сервер администрирования не перечисляет устройство среди управляемых устройств. Вам потребуется убедиться, что Сервер администрирования инициировал соединение со шлюзом соединения.

- `This device is a connection gateway` – утилита klnagchk запускается на устройстве, которое выполняет роль шлюза соединения.

- `Acts as a distribution point` – утилита klnagchk запускается на устройстве, которое выполняет роль точки распространения.

Утилита klnagchk проверяет состояние службы Агента администрирования. Если служба не запущена, утилита останавливается. Если служба запущена, утилита отображает следующую статистику подключений:

- `Ping count` – количество попыток подключения клиентского устройства к Серверу администрирования.

- `Succ. pings` – количество успешных попыток подключения клиентского устройства к Серверу администрирования.

- `Sync count` – количество попыток синхронизации параметров клиентского устройства с параметрами Сервера администрирования.

- `Succ. syncs` – количество успешных попыток синхронизации параметров клиентского устройства с Сервером администрирования.

- `Last ping` – дата и время последнего подключения.

При анализе соединения между Сервером администрирования и Агентом администрирования необходимо использовать параметры `Ping count` и `Succ. pings`. Параметры клиентского устройства синхронизируются с параметрами Сервера администрирования только в случае изменения параметров Сервера администрирования (например, при добавлении новых задач или изменении параметров политики). Иначе значения параметров `Ping count` и `Succ. pings` не изменяются.

Подробнее об устранении проблем с подключением Агента администрирования к Серверу администрирования см. Open Single Management Platform FAQ.

Выборки устройств

Выборки устройств – это инструмент для фильтрации устройств в соответствии с заданными условиями. Вы можете использовать выборки устройств, чтобы управлять несколькими устройствами: например, для просмотра отчетов только о выбранных устройствах или для перемещения всех этих устройств в другую группу администрирования.

Open Single Management Platform предоставляет широкий диапазон *предопределенных выборок устройств* (например, **Устройства со статусом "Критический"**, **Защита выключена**, **Обнаружены активные угрозы**). Предопределенные выборки невозможно удалить. Вы можете также создавать и настраивать дополнительные *пользовательские выборки событий*.

В пользовательских выборках вы можете задать область поиска и выбрать все устройства, управляемые устройства или нераспределенные устройства. Параметры поиска задаются в условиях. В выборках устройств вы можете создать несколько условий с различными параметрами поиска. Например, вы можете создать два условия и задать различные IP-диапазоны в каждом из них. Если задано несколько условий, в выборку устройств попадут устройства, которые удовлетворяют любому из условий. Напротив, параметры поиска в одном условии накладываются друг на друга. Если в условии выборки заданы IP-диапазон и название установленного приложения, то в выборку устройств попадут только те устройства, на которых одновременно установлено указанное приложение и их IP-адреса входят в указанный диапазон.

Просмотр списка устройств из выборки устройств

Open Single Management Platform позволяет просматривать список устройств из выборки устройств.

Чтобы просмотреть список устройств из выборки устройств:

1. В главном окне приложения перейдите в раздел **Управление активами → Выборки устройств** или в раздел **Обнаружение устройств и развертывание → Выборки устройств**.

2. В списке выборок нажмите на имя выборки устройств.

   На странице отображается таблица с информацией об устройствах, включенных в выборку устройств.

3. Вы можете группировать и фильтровать данные таблицы устройств следующим образом:

   - Нажмите на значок параметров (⚙) и выберите столбцы для отображения в таблице.
   - Нажмите на значок фильтрации ( ), укажите и примените критерий фильтрации в открывшемся меню.

     Отобразится отфильтрованная таблица устройств.

Также вы можете запускать задачи для устройств выборки. Для этого выберите одно или несколько устройств, затем нажмите на кнопку **Запустить задачу** и выберите: **Создать задачу**, которая будет применена к этим устройствам, либо **Использовать существующую задачу**.

Чтобы переместить выбранные устройства из выборки устройств в другую группу администрирования, нажмите на кнопку **Переместить в группу** и выберите целевую группу администрирования.

Создание выборки устройств

Чтобы создать выборку устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Выборки устройств**.

   Отобразится страница со списком выборок устройств.

2. Нажмите на кнопку **Добавить**.

   Откроется окно **Параметры выборки устройств**.

3. Введите имя новой выборки.

4. Укажите группу, содержащую устройства, которые будут включены в выборку устройств:

   - **Искать любые устройства** – поиск устройств, соответствующих критериям выборки, в группах **Управляемые устройства** или **Нераспределенные устройства**.
   - **Искать управляемые устройства** – поиск устройств, соответствующих критериям выборки, в группе **Управляемые устройства**.
   - **Искать нераспределенные устройства** – поиск устройств, соответствующих критериям выборки, в группе **Нераспределенные устройства**.

   Вы можете установить флажок **Включать данные подчиненных Серверов администрирования**, чтобы включить поиск устройств, отвечающих критериям выборки, на подчиненных Серверах администрирования.

5. Нажмите на кнопку **Добавить**.

6. В открывшемся окне укажите условия, которые должны быть выполнены для включения устройств в эту выборку и нажмите на кнопку **Сохранить**.

7. Нажмите на кнопку **Сохранить**.

Выборка устройств создана и добавлена в список выборок устройств.

Настройка выборки устройств

Чтобы настроить параметры выборки устройств:

1. В главном окне приложения перейдите в раздел **Управление активами → Выборки устройств**.

   Отобразится страница со списком выборок устройств.

2. Выберите соответствующую пользовательскую выборку устройств и нажмите на кнопку **Свойства**.

   Откроется окно **Параметры выборки устройств**.

3. На вкладке **Общие** перейдите по ссылке **Новое условие**.

4. Укажите условия, которые должны быть выполнены, чтобы устройство было включено в эту выборку.

5. Нажмите на кнопку **Сохранить**.

   Параметры применены и сохранены.

Ниже описаны параметры условий отнесения устройств к выборке. Условия сочетаются по логическому "или": в выборку попадают устройства, удовлетворяющие хотя бы одному из представленных условий.

Общие

В разделе **Общие** можно изменить имя условия выборки и указать, необходимо ли инвертировать это условие:

Инвертировать условие выборки

По умолчанию параметр выключен.

Если вы включите этот параметр, заданное условие выборки будет инвертировано. В выборку попадут все устройства, не соответствующие условию.

В следующем примере показана логика работы инверсии:

- **Условие**: на вашем устройстве установлена операционная система с типом Linux и номером сборки 00.0.000.
- **Инвертированное состояние**: на вашем устройстве установлена операционная система с НЕ (тип Linux и номер сборки 00.0.000), что эквивалентно следующему:

  Есть операционная система с типом НЕ Linux ИЛИ с номером сборки НЕ 00.0.000.

Таким образом, выборка будет включать устройства с операционной системой, например, с типом Windows и номером сборки 00.0.000 или типом Linux и любым номером сборки, отличным от 00.0.000.

Инфраструктура сети

В разделе **Сеть** можно настроить критерии включения устройств в выборку на основании их сетевых данных:

- **Имя устройства**

  Имя устройства в сети Windows (NetBIOS-имя) или IPv4-адрес или IPv6-адрес.

- **Домен**

  Отображаются все устройства, входящие в указанную рабочую группу.

- **Группа администрирования**

  Будут отображаться устройства, входящие в указанную группу администрирования.

- **Описание**

  Текст, который содержится в окне свойств устройства: в поле **Описание** раздела **Общие**.

  Для описания текста в поле **Описание** допустимо использовать следующие символы:

  - Внутри одного слова:

    - *****. Заменяет любую строку длиной 0 и более символов.

    Пример:

    Для описания слов **Сервер**, **Серверный** или Серверная можно использовать строку **Сервер***.

    - **?.** Заменяет любой один символ.

    Пример:

    Для описания таких фраз, как **SUSE Linux корпоративный сервер 12** или же **SUSE Linux корпоративный сервер 15**, можно ввести **SUSE Linux Enterprise Server 1?**.

    Звездочка (*****) или вопросительный знак (**?**) не могут использоваться как первый символ в описании текста.

  - Для связи нескольких слов:

    - Пробел. Отображает все устройства, описания которых содержат любое из перечисленных слов.

    Пример:

    Для описания фразы, содержащей слово **Подчиненный** или **Виртуальный** можно использовать строку **Подчиненный Виртуальный**.

    - **+**. При написании перед словом обозначает обязательное наличие слова в тексте.

    Пример:

    Для описания фразы, содержащей и слово **Подчиненный**, и слово **Виртуальный**, можно использовать строку **+Подчиненный+Виртуальный**.

    - **-**. При написании перед словом обозначает обязательное отсутствие слова в тексте.

    Пример:

    Для описания фразы, в которой должно присутствовать слово **Подчиненный**, но должно отсутствовать слово **Виртуальный**, можно использовать строку **+Подчиненный-Виртуальный**.

    - **"<фрагмент текста>"**. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте.

    Пример:

    Для описания фразы, содержащей словосочетание **Подчиненный Сервер**, можно использовать строку **"Подчиненный Сервер"**.

- **IP-диапазон**

  Если этот параметр включен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

По умолчанию параметр выключен.

- **Под управлением другого Сервера администрирования**

  Выберите одно из следующих значений:

  - **Да**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым другими Серверами администрирования. Эти Серверы отличаются от Сервера, на котором вы настраиваете правило перемещения устройств.
  - **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым текущим Сервером администрирования.
  - **Значение не выбрано**. Условие не применяется.

В разделе **Active Directory** можно настроить критерии включения устройств в выборку на основании их данных Active Directory:

- **Устройство в подразделении Active Directory**

  Если этот параметр включен, в выборку будут включаться устройства из организационной единицы Active Directory, указанного в поле ввода.

  По умолчанию параметр выключен.

- **Включать дочерние подразделения**

  Если этот параметр включен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы контроллера домена.

  По умолчанию параметр выключен.

- **Устройство является членом группы Active Directory**

  Если этот параметр включен, в выборку будут включаться устройства из группы Active Directory, указанной в поле ввода.

  По умолчанию параметр выключен.

В разделе **Действия в сети** можно настроить критерии включения устройств в выборку на основании их сетевой активности:

- **Является точкой распространения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. В выборку будут включены устройства, являющиеся точками распространения.
  - **Нет**. Устройства, являющиеся точками распространения, не будут включены в выборку.
  - **Значение не выбрано**. Критерий не применяется.

- **Не разрывать соединение с Сервером администрирования**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Включен**. Выборка будет включать устройства, для которых установлен флажок **Не разрывать соединение с Сервером администрирования**.
  - **Выключен**. Выборка будет включать устройства, для которых снят флажок **Не разрывать соединение с Сервером администрирования**.
  - **Значение не выбрано**. Критерий не применяется.

- **Переключение профиля подключения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. В выборку будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
  - **Нет**. В выборку не будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
  - **Значение не выбрано**. Критерий не применяется.

- **Последнее подключение к Серверу администрирования**

  С помощью этого флажка можно задать критерий поиска устройств по времени последнего соединения с Сервером администрирования.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее соединение установленного на клиентском устройстве Агента администрирования с Сервером администрирования. В выборку будут включены устройства, соответствующие установленному интервалу.

  Если флажок снят, то критерий не применяется.

  По умолчанию флажок снят.

- **Новые устройства, обнаруженные при опросе сети**

  Поиск новых устройств, обнаруженных при опросе сети за последние несколько дней.

  Если этот параметр включен, то в выборку попадают только новые устройства, найденные в процессе обнаружения устройств за количество дней, которое указано в поле **Период обнаружения (сут)**.

  Если этот параметр выключен, то в выборку попадают все устройства, найденные в процессе обнаружения устройств.

  По умолчанию параметр выключен.

- **Устройство в сети**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. Приложение включает в выборку устройства, которые видимы в сети в настоящий момент.
  - **Нет**. Приложение включает в выборку устройства, которые не видимы в сети в настоящий момент.
  - **Значение не выбрано**. Критерий не применяется.

В разделе **Облачные сегменты** можно настроить критерии включения устройств в выборку в соответствии с облачными сегментами:

- **Устройство находится в облачном сегменте**

  Если этот параметр включен, вы можете выбрать устройства из облачных сегментов AWS, Azure и Google.

  Если также включен параметр **Включать дочерние объекты**, то поиск ведется по всем вложенным объектам указанного сегмента.

  В результаты поиска включаются устройства только из выбранного сегмента.

- **Устройство обнаружено с помощью API**

  В раскрывающемся списке можно выбрать, обнаруживается ли устройство средствами API:

  - **Да**. Устройство обнаруживается с помощью AWS, Azure или Google API.
  - **Нет**. Устройство не обнаруживается с помощью AWS, Azure или Google API. То есть устройство либо находится вне облачного окружения, либо находится в облачном окружении, но по каким-то причинам недоступно для поиска с помощью API.
  - Не задано. Это условие не применяется.

Статусы устройств

В разделе **Статус управляемых устройств** можно настроить критерии включения устройств в выборку по описанию статуса устройства от управляемого приложения:

- **Статус устройства**

  Раскрывающийся список, в котором можно выбрать один из статусов устройства: *OK*, *Критический* или *Предупреждение*.

- **Статус постоянной защиты**

  Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

- **Device status description**

  В этом поле можно установить флажки для условий, при соблюдении которых устройству будет присваиваться выбранный статус: *OK, Критический* или *Предупреждение*.

В разделе **Статусы компонентов управляемых приложений** можно настроить критерии включения устройств в выборку по статусам компонентов управляемых приложений:

- **Статус защиты данных от утечек**

  Поиск устройств по статусу компонента защиты от утечки данных (*Нет данных, Остановлена, Запускается, Приостановлена, Выполняется, Сбой*).

- **Статус защиты для серверов совместной работы**

  Поиск устройств по статусу защиты для серверов совместной работы (*Нет данных*, *Остановлена*, *Запускается, Приостановлена*, *Выполняется*, *Сбой*).

- **Статус антивирусной защиты почтовых серверов**

  Поиск устройств по статусу защиты почтовых серверов (*Нет данных, Остановлена, Запускается, Приостановлена, Выполняется, Сбой*).

- **Статус Endpoint Sensor**

  Поиск устройств по статусу компонента Endpoint Sensor (*Нет данных, Остановлена, Запускается, Приостановлена, Выполняется, Сбой*).

В разделе **Проблемы, связанные со статусом управляемых приложений** можно настроить критерии включения устройств в выборку в соответствии со списком возможных проблем, обнаруженных управляемым приложением. Если на устройстве существует хотя бы одна проблема, которую вы выбирали, устройство будет включено в выборку. Когда вы выбираете проблему, указанную для нескольких приложений, у вас есть возможность автоматически выбрать эту проблему во всех списках.

Вы можете установить флажки для описаний статусов от управляемого приложения, при получении которых устройства будут включаться в выборку. Когда вы выбираете статус, указанный для нескольких приложений, у вас есть возможность автоматически выбирать этот статус во всех списках.

Сведения о системе

В разделе **ОС** можно настроить критерии включения устройств в выборку на основании установленной на них операционной системы.

- **Тип платформы**

  Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются в результаты поиска.

- **Версия пакета обновления ОС**

  В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- **Архитектура ОС**

  В раскрывающемся списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Нет данных**, **x86**, **AMD64** или **IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

- **Сборка ОС**

  > Этот параметр применим только для операционных систем Windows.

  Номер сборки операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить поиск всех номеров сборки, кроме указанного.

- **Номер выпуска ОС**

  > Этот параметр применим только для операционных систем Windows.

Идентификатор выпуска операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний идентификатор выпуска. Вы также можете настроить поиск всех номеров идентификаторов выпуска, кроме указанного.

В разделе **Виртуальные машины** можно настроить критерии включения устройств в выборку в зависимости от того, являются эти устройства виртуальными машинами или частью Virtual Desktop Infrastructure:

- **Является виртуальной машиной**

  В раскрывающемся списке можно выбрать следующие элементы:

  - **Не определено**.
  - **Нет**. Искомые устройства не должны являться виртуальными машинами.
  - **Да**. Искомые устройства должны являться виртуальными машинами.

- **Тип виртуальной машины**

  В раскрывающемся списке можно выбрать производителя виртуальной машины.

  Этот список доступен, если в раскрывающемся списке **Является виртуальной машиной** выбрано значение **Да** или **Неважно**.

- **Часть Virtual Desktop Infrastructure**

  В раскрывающемся списке можно выбрать следующие элементы:

  - **Не определено**.
  - **Нет**. Искомые устройства не должны являться частью Virtual Desktop Infrastructure.
  - **Да**. Искомые устройства должны являться частью Virtual Desktop Infrastructure (VDI).

В разделе **Реестр оборудования** можно настроить критерии включения устройств в выборку по установленному на них оборудованию:

Убедитесь, что утилита lshw установлена на устройствах Linux, с которых вы хотите получить информацию об оборудовании. Сведения об оборудовании, полученные с виртуальных машин, могут быть неполными в зависимости от используемого гипервизора

- **Устройство**

  В раскрывающемся списке можно выбрать тип оборудования. Все устройства с таким оборудованием включены в результат поиска.

  В поле поддерживается полнотекстовый поиск.

- **Поставщик**

  В раскрывающемся списке можно выбрать имя производителя оборудования. Все устройства с таким оборудованием включены в результат поиска.

  В поле поддерживается полнотекстовый поиск.

- **Имя устройства**

  Устройство с указанным именем будет включено в выборку.

- **Описание**

  Описание устройства или оборудования. Устройства с описанием, указанным в поле, будут включены в состав выборки.

  Описание устройства в произвольной форме можно ввести в окне свойств устройства. В поле поддерживается полнотекстовый поиск.

- **Поставщик устройства**

  Название производителя устройства. Устройства, изготовленные производителем, указанным в поле, будут включены в состав выборки.

  Название производителя можно ввести в окне свойств устройства.

- **Серийный номер**

  Оборудование с серийным номером, указанным в поле, будет включено в выборку.

- **Инвентарный номер**

  Оборудование с инвентарным номером, указанным в поле, будет включено в выборку.

- **Пользователь**

  Оборудование пользователя, указанного в поле, будет включено в выборку.

- **Расположение**

  Место расположения устройства или оборудования (например, в офисе или филиале). Компьютеры или другие устройства с расположением, указанным в поле, будут включены в состав выборки.

  Расположение оборудования в произвольной форме можно ввести в окне свойств оборудования.

- **Частота процессора (МГц) от**

  Минимальная тактовая частота процессора. Устройства с процессорами, соответствующими диапазону тактовой частоты, указанному в полях ввода (включительно), будут включены в состав выборки.

- **Частота процессора (МГц) до**

  Максимальная тактовая частота процессора. Устройства с процессорами, соответствующими диапазону тактовой частоты, указанному в полях ввода (включительно), будут включены в состав выборки.

- **Количество виртуальных ядер процессора от**

  Минимальное количество виртуальных ядер CPU. Устройства с процессорами, соответствующими диапазону количества виртуальных ядер, указанному в полях ввода (включительно), будут включены в состав выборки.

- **Количество виртуальных ядер процессора до**

  Максимальное количество виртуальных ядер CPU. Устройства с процессорами, соответствующими диапазону количества виртуальных ядер, указанному в полях ввода (включительно), будут включены в состав выборки.

- **Объем жесткого диска (ГБ), от**

  Минимальный объем жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону значений в полях ввода (включительно), будут включены в состав выборки.

- **Объем жесткого диска (ГБ), до**

  Максимальный объем жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону значений в полях ввода (включительно), будут включены в состав выборки.

- **Объем оперативной памяти (МБ) от**

  Минимальный объем оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону значений в полях ввода (включительно), будут включены в состав выборки.

- **Объем оперативной памяти (МБ) до**

  Максимальный объем оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону значений в полях ввода (включительно), будут включены в состав выборки.

Информация о приложениях сторонних производителей

В разделе **Реестр приложений** можно настроить критерии включения устройств в выборку в зависимости от того, какие приложения на них установлены:

- **Название приложения**

  Раскрывающийся список, в котором можно выбрать приложение. Устройства, на которых установлено указанное приложение, будут включены в выборку.

- **Версия приложения**

  Поле ввода, в котором указывается версия выбранного приложения.

- **Поставщик**

  Раскрывающийся список, в котором можно выбрать производителя установленного на устройстве приложения.

- **Статус приложения**

  Раскрывающийся список, в котором можно выбрать статус приложения (*Установлено*, *Не установлено*). Устройства, на которых указанное приложение установлено или не установлено, в зависимости от выбранного статуса, будут включены в выборку.

- **Искать по обновлению**

  Если этот параметр включен, поиск будет выполняться по данным об обновлении приложений, установленных на искомых устройствах. После установки этого флажка вместо полей **Название приложения**, **Версия приложения** и **Статус приложения** будут отображаться поля **Имя обновления**, **Версия обновления** и **Статус** соответственно.

  По умолчанию параметр выключен.

- **Название несовместимого приложения безопасности**

  Раскрывающийся список, в котором можно выбрать приложения безопасности сторонних производителей. Во время поиска устройства, на которых установлено выбранное приложение, будут включены в выборку.

- **Тег приложения**

  В раскрывающемся списке можно выбрать тег приложения. Все устройства, на которых установлены приложения, имеющие выбранный тег в описании, включаются в выборку устройств.

- **Применить к устройствам без выбранных тегов**

  Если параметр включен, в выборку будут включены устройства, в описании которых нет выбранных тегов.

  Если этот параметр выключен, критерий не применяется.

  По умолчанию параметр выключен.

В разделе **Уязвимости и обновления** можно настроить критерии включения устройств в выборку по источнику обновлений Центра обновления Windows:

WUA переключен на Сервер администрирования

В раскрывающемся списке можно выбрать один из следующих вариантов поиска:

- **Да**. Если выбран этот вариант, в результаты поиска включаются устройства, которые получают обновления Центра обновления Windows с Сервера администрирования.
- **Нет**. Если выбран этот вариант, в результаты включаются устройства, которые получают обновления Центра обновления Windows из другого источника.

Информация о приложениях "Лаборатории Касперского"

В разделе **Приложения "Лаборатории Касперского"** можно настроить критерии включения устройств в выборку на основании выбранного управляемого приложения:

- **Название приложения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске по наименованию приложения "Лаборатории Касперского".

  В списке представлены названия только тех приложений, для которых на рабочем месте администратора установлены плагины управления.

  Если приложение не выбрано, то критерий не применяется.

- **Версия приложения**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии приложения "Лаборатории Касперского".

  Если номер версии не указан, то критерий не применяется.

- **Название критического обновления**

  Раскрывающийся список, в котором можно выбрать статус приложения (*Установлено*, *Не установлено*). Устройства, на которых указанное приложение установлено или не установлено, в зависимости от выбранного статуса, будут включены в выборку.

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для приложения наименованию или номеру пакета обновления.

  Если поле не заполнено, то критерий не применяется.

- **Выбор периода последнего обновления модулей**

  С помощью этого параметра можно задать критерий поиска устройств по времени последнего обновления модулей приложений, установленных на устройствах.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее обновление модулей приложений, установленных на устройствах.

  Если флажок снят, то критерий не применяется.

По умолчанию флажок снят.

- **Устройство находится под управлением Сервера администрирования**

  В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky SIEM Cloud:

  - **Да**. Приложение включает в выборку устройства, которые находятся под управлением Kaspersky SIEM Cloud.
  - **Нет**. Приложение включает в выборку устройства, которые не находятся под управлением Kaspersky SIEM Cloud.
  - **Значение не выбрано**. Критерий не применяется.

- **Приложение безопасности установлено**

  В раскрывающемся списке можно включить в состав выборки устройства, на которых установлено приложение безопасности:

  - **Да**. Приложение включает в выборку устройства, на которых установлено приложение безопасности.
  - **Нет**. Приложение включает в выборку устройства, на которых не установлено приложение безопасности.
  - **Значение не выбрано**. Критерий не применяется.

В разделе **Антивирусная защита** можно настроить критерии включения устройств в выборку по состоянию защиты:

- **Дата выпуска баз**

  Если этот параметр выбран, поиск клиентских устройств выполняется по дате выпуска антивирусных баз. В полях ввода можно задать временной интервал, на основании которого будет выполняться поиск.

  По умолчанию параметр выключен.

- **Количество записей в базах**

  Если этот параметр включен, поиск клиентских устройств выполняется по количеству записей в базе. В полях ввода можно задать нижнее и верхнее значения количества записей антивирусной базы.

  По умолчанию параметр выключен.

- **Последняя проверка**

  Если этот параметр включен, поиск клиентских устройств выполняется по времени последнего поиска вредоносного ПО. В полях ввода можно указать интервал, в течение которого поиск вредоносного ПО выполнялся в последний раз.

  По умолчанию параметр выключен.

- **Обнаружены угрозы**

  Стандарт симметричного алгоритма блочного шифрования Advanced Encryption Standard (AES). В раскрывающемся списке вы можете выбрать размер ключа шифрования (56 Бит, 128 Бит, 192 Бит или 256 Бит).

  Доступные значения: *AES56*, *AES128*, *AES192*, и *AES256*.

Если этот параметр включен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

По умолчанию параметр выключен.

Подраздел **Компоненты приложения** содержит список компонентов тех приложений, которые имеют соответствующие плагины управления, установленные в OSMP Console.

В разделе **Компоненты приложения** вы можете задать критерий для включения устройств в выборку в соответствии с номерами версий компонентов, относящихся к выбранному приложению:

- **Статус**

  Поиск устройств в соответствии со статусом компонента, отправленным управляемым приложением на Сервер администрирования. Вы можете выбрать один из следующих статусов: *Нет данных от устройства, Остановлен*, *Приостановлено*, *Запускается*, *Выполняется*, *Сбой*, *Не установлен, Не поддерживается лицензией*. Если выбранный компонент приложения, установленный на управляемом устройстве, имеет указанный статус, устройство входит в выборку устройств.

  Статусы, отправленные приложениями:

  - *Остановлено* – компонент отключен и в данный момент не работает.
  - *Приостановлено* – компонент приостановлен, например, после того, как пользователь приостановил защиту в управляемом приложении.
  - *Запускается* – компонент в настоящее время находится в процессе инициализации.
  - *Выполняется* – компонент включен и работает правильно.
  - *Сбой* – во время выполнения операции компонента произошла ошибка.
  - *Не установлено* – пользователь не выбрал компонент для установки во время выборочной установки приложения.
  - *Не поддерживается лицензией* – лицензия не распространяется на выбранный компонент.

  В отличие от других статусов, статус *Нет данных от устройства* не отправляется управляемым приложением. Этот параметр показывает, что приложения не имеют информации о выбранном статусе компонента. Например, это может произойти, если выбранный компонент не принадлежит ни одному из приложений, установленных на устройстве, или устройство выключено.

- **Версия**

  Поиск устройств в соответствии с номером версии компонента, который вы выбрали в списке. Вы можете ввести номер версии, например, `3.4.1.0`, а затем указать, должен ли выбранный компонент иметь равную, более раннюю или более позднюю версию. Также вы можете настроить поиск по всем версиям компонента, кроме указанной.

Теги

В разделе **Теги** можно настроить критерии включения устройств в выборку по ключевым словам (тегам), которые были добавлены ранее в описания управляемых устройств:

Применить, если есть хотя бы один из выбранных тегов

Если этот параметр включен, в результатах поиска отобразятся устройства, в описании которых есть хотя бы один из выбранных тегов.

Если этот параметр выключен, в результатах поиска отобразятся только устройства, в описаниях которых есть все выбранные теги.

По умолчанию параметр выключен.

Чтобы добавить теги к критерию, нажмите на кнопку **Добавить** и выберите теги, нажав на поле ввода **Тег**. Укажите, следует ли включать или исключать устройства с выбранными тегами в выборку устройств.

- **Все устройства, имеющие этот тег**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

  По умолчанию выбран этот вариант.

- **Все устройства, не имеющие этого тега**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

Пользователи

В разделе **Пользователи** можно настроить критерии включения устройств в выборку по учетным записям пользователей, выполнявших вход в операционную систему.

- **Последний пользователь, выполнивший вход в систему**

  Если этот параметр включен, вы можете выбрать учетную запись пользователя, для которой настроили критерий. В результаты поиска включаются устройства, на которых последний вход в систему выполнялся выбранным пользователем.

- **Пользователь, уже выполнявший вход в систему**

  Если этот параметр включен, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

Экспорт списка устройств из выборки устройств

Open Single Management Platform позволяет сохранять информацию об этих устройствах из выборки устройств и экспортировать ее в файл CSV или TXT.

Чтобы экспортировать список устройств из выборки устройств:

1. Откройте таблицу с устройствами из выборки устройств.
2. Используйте один из следующих способов для выбора устройств, которые вы хотите экспортировать:
   - Чтобы выбрать определенные устройства, установите флажки рядом с ними.
   - Чтобы выбрать все устройства на текущей странице таблицы, установите флажок в заголовке таблицы устройств, а затем установите флажок **Выбрать все на текущей странице**.
   - Чтобы выбрать все устройства из таблицы, установите флажок в заголовке таблицы устройств, а затем выберите **Выбрать все**.

Нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**. Вся информация о выбранных устройствах, включенных в таблицу, будет экспортирована.

Обратите внимание, если вы отфильтровали таблицу устройств, будут экспортированы только отфильтрованные данные отображаемых столбцов.

Удаление устройств из групп администрирования в выборке

При работе с выборкой устройств вы можете удалять устройства из групп администрирования прямо в выборке, не переходя к работе с группами администрирования, из которых требуется удалить устройства.

Чтобы удалить устройства из групп администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Выборки устройств** или **Обнаружение устройств и развертывание** → **Выборки устройств**.
2. В списке выборок нажмите на имя выборки устройств.

   На странице отображается таблица с информацией об устройствах, включенных в выборку устройств.
3. Выберите устройства, которые вы хотите удалить и нажмите на кнопку **Удалить**.

   В результате выбранные устройства будут удалены из групп администрирования, в которые они входили.

Просмотр и настройка действий, когда устройство неактивно

Если клиентские устройства группы администрирования неактивны, вы можете получать уведомления об этом. Вы также можете автоматически удалять такие устройства.

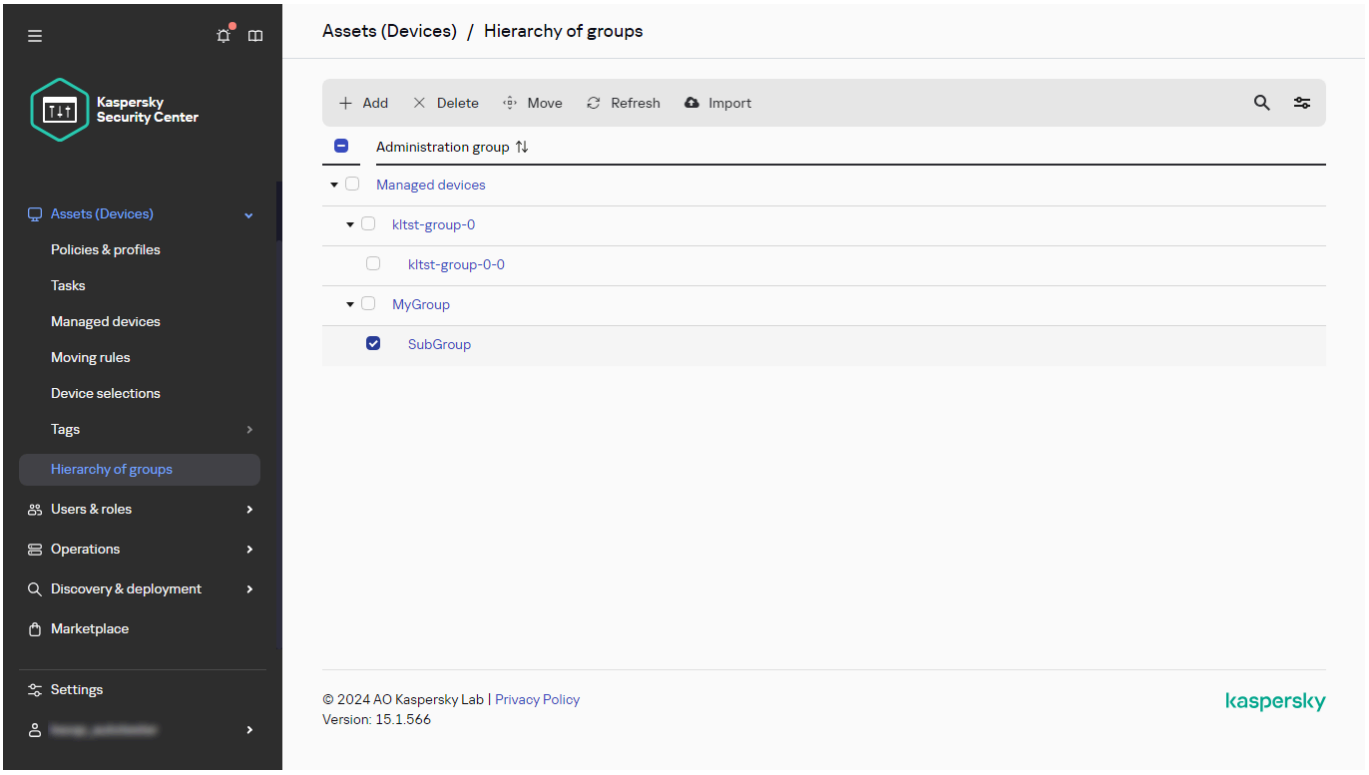
Чтобы просмотреть или настроить действия, когда устройства неактивны в группе администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.

2. Перейдите к свойствам нужной группы администрирования одним из следующих способов:

   - Выберите имя группы администрирования.

   - Нажмите на кнопку **Показать иерархию** в верхней части страницы. В открывшейся панели наведите курсор мыши на название нужной группы и нажмите на значок параметров (⚙).



Иерархия групп администрирования

   Откроется окно свойств группы администрирования.

3. В окне свойств перейдите на вкладку **Параметры**.

4. В разделе **Наследование** включите или выключите следующие параметры:

   Наследовать из родительской группы

   Если флажок установлен, параметры в этом разделе будут наследоваться из родительской группы, в которую входит клиентское устройство. Если флажок установлен, параметры в блоке параметров **Активность устройств в сети** недоступны для изменения.

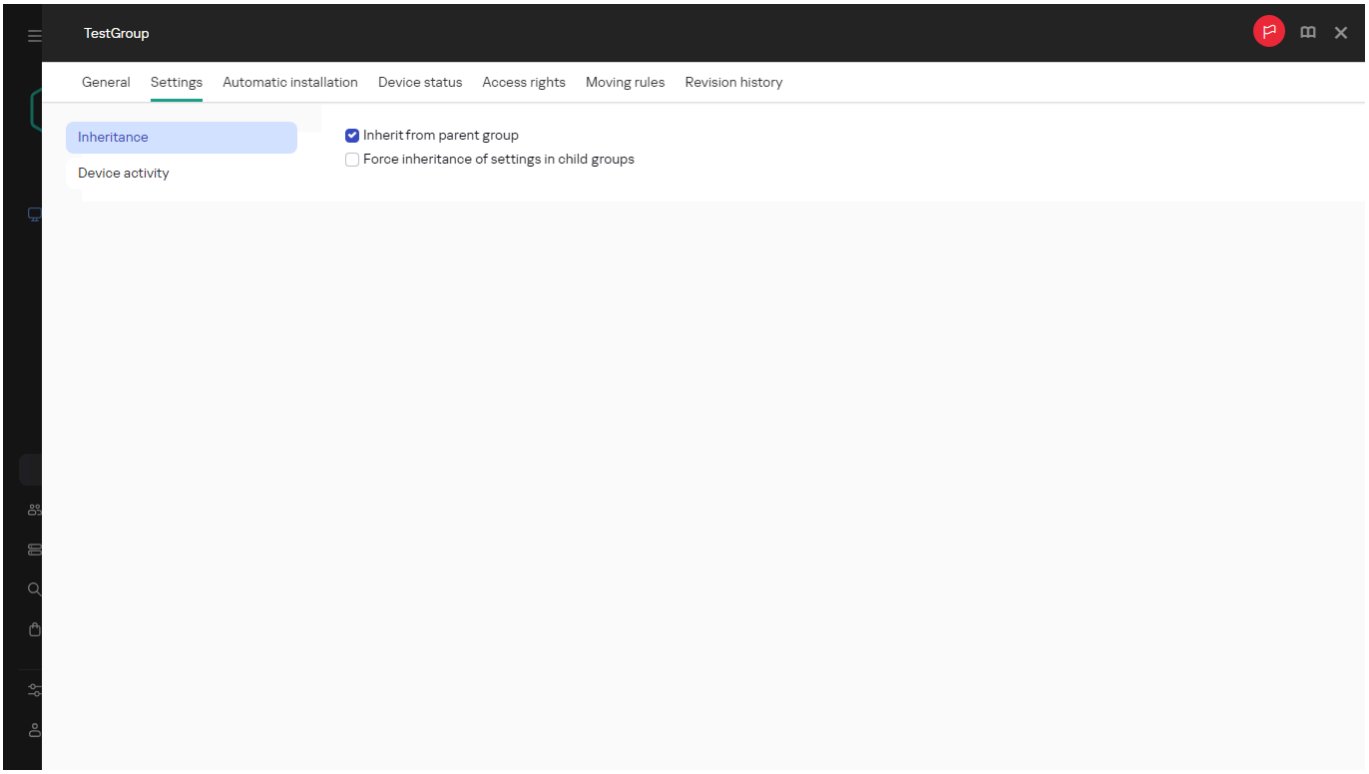
   Этот параметр доступен только для группы администрирования, у которой есть родительская группа администрирования.

   По умолчанию параметр включен.

   Обеспечить принудительное наследование параметров для дочерних групп

   Значения параметров будут распределены по дочерним группам, но в свойствах дочерних групп эти параметры недоступны для изменений.

   По умолчанию параметр выключен.



Свойства группы администрирования

5. В разделе **Активность устройств** включите или выключите следующие параметры:

   Уведомлять администратора, если устройство неактивно больше (сут)

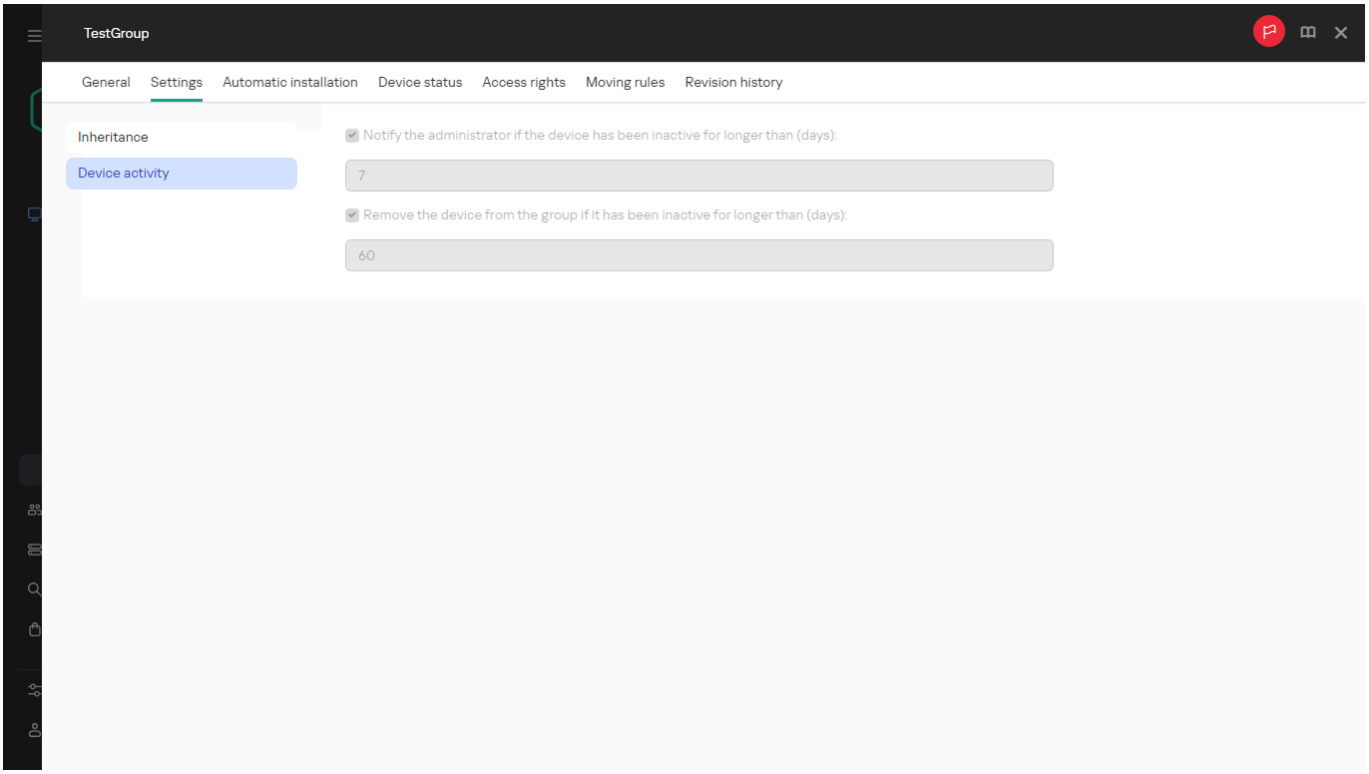
   Если этот параметр включен, администратор получает уведомления о неактивности устройств. В поле ввода можно задать интервал времени, по истечении которого будет сформировано событие **Устройство долго не проявляет активности в сети**. Временной интервал, установленный по умолчанию, составляет 7 дней.

   По умолчанию параметр включен.

   Удалять устройство из группы, если оно неактивно больше (сут)

   Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. Временной интервал, установленный по умолчанию, составляет 60 дней.

По умолчанию параметр включен.



Свойства группы администрирования

6. Нажмите на кнопку **Сохранить**.

Ваши изменения сохранены и применены.

О статусах устройства

Kaspersky SIEM Cloud присваивает статус каждому управляемому устройству. Конкретный статус зависит от того, выполнены ли условия, определенные пользователем. В некоторых случаях при присваивании статуса устройству Kaspersky SIEM Cloud учитывает видимость устройства в сети (см. таблицу ниже). Если Kaspersky SIEM Cloud не находит устройство в сети в течение двух часов, видимость устройства принимает значение *Не в сети*.

Существуют следующие статусы:

- *Критический* или *Критический/Видим в сети*.
- *Предупреждение* или *Предупреждение/Видим в сети*.
- *OK* или *OK/Видим в сети*.

В таблице ниже приведены условия по умолчанию для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения.

Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Приложение безопасности не установлено	Агент администрирования установлен на устройстве, но не установлено приложение безопасности.	• Переключатель включен. • Переключатель выключен.

Условие	Описание условия	Доступные значения
Обнаружено много вирусов	В результате работы задач поиска вирусов, например, задачи Поиск вирусов, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.	Более 0.
Уровень постоянной защиты отличается от уровня, установленного администратором	Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	• Остановлена. • Приостановлена. • Выполняется.
Давно не выполнялся поиск вредоносного ПО	Устройство видимо в сети и на устройстве установлено приложение безопасности, но ни задача *Поиск вредоносного ПО*, ни задача локальной проверки не выполнялись больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня.
Базы устарели	Устройство видимо в сети и на устройстве установлено приложение безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня.
Давно не подключались	Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.	Более 1 дня.
Обнаружены активные угрозы	Количество необработанных объектов в папке **Активные угрозы** превышает указанное значение.	Более чем 0 штук.
Требуется перезагрузка	Устройство видимо в сети, но приложение требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин.	Более чем 0 минут.
Установлены несовместимые приложения	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые приложения.	• Переключатель выключен. • Переключатель включен.
Обнаружены уязвимости в приложениях	Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи *Поиск уязвимостей и требуемых обновлений* на устройстве обнаружены уязвимости в приложениях с заданным уровнем критичности.	• Предельный. • Высокий. • Средний. • Игнорировать, если невозможно закрыть уязвимость. • Игнорировать, если обновление назначено к установке.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	• Переключатель выключен. • Переключатель включен.
Срок действия лицензии скоро истекает	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Менее чем 0 дней.

Условие	Описание условия	Доступные значения
Давно не выполнялась проверка обновлений Центра обновления Windows	Устройство видимо в сети, но задача *Поиск уязвимостей и требуемых обновлений* не выполнялась больше указанного времени.	Более 1 дня.
Недопустимый статус шифрования	Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению.	• Не соответствует политике из-за отказа пользователя (только для внешних устройств). • Не соответствует политике из-за ошибки. • В процессе применения политики – требуется перезагрузка. • Не задана политика шифрования. • Не поддерживается. • В процессе применения политики.
Параметры мобильного устройства не соответствуют политике	Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия.	• Переключатель выключен. • Переключатель включен.
Есть необработанные проблемы безопасности	На устройстве есть необработанные проблемы безопасности. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором.	• Переключатель выключен. • Переключатель включен.
Статус устройства определен приложением	Статус устройства определяется управляемым приложением.	• Переключатель выключен. • Переключатель включен.
На устройстве заканчивается дисковое пространство	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *OK*, когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению.	Более чем 0 МБ
Устройство стало неуправляемым	Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	• Переключатель выключен. • Переключатель включен.
Защита выключена	Устройство видимо в сети, но приложение безопасности на устройстве отключено больше указанного времени. В этом случае состояние приложения безопасности *Остановлено* или *Сбой* и отличается от следующих: *Запускается*, *Выполняется* или *Приостановлено*.	Более чем 0 минут.
Приложение безопасности не запущено	Устройство видимо в сети и приложение безопасности установлено на устройстве, но не запущено.	• Переключатель выключен. • Переключатель включен.

Kaspersky SIEM Cloud позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*. При невыполнении заданных условий клиентскому устройству присваивается статус *OK*.

Разным значениям одного условия могут соответствовать разные статусы. Например, по умолчанию при соблюдении условия **Базы устарели** со значением **Более 3 дней** клиентскому устройству присваивается статус *Предупреждение*, а со значением **Более 7 дней** – статус *Критический*.

Когда Kaspersky SIEM Cloud присваивает устройству статус, для некоторых условий (см. столбец "Описание условий") учитывается видимость устройств в сети. Например, если управляемому устройству был присвоен статус *Критический*, так как выполнено условие Базы устарели, а затем для устройства стало видимо в сети, то устройству присваивается статус *OK*.

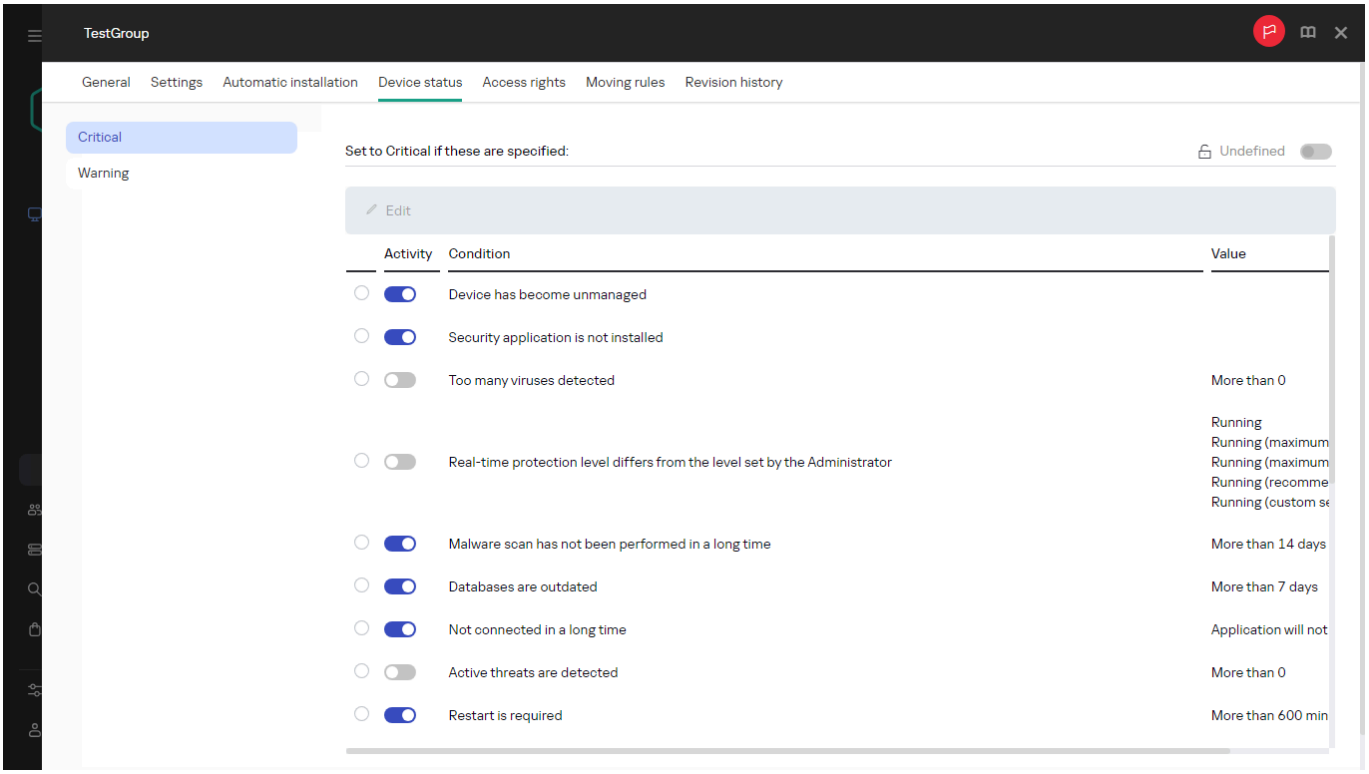
Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

Чтобы изменить статус устройства на Критический:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.
2. Перейдите в свойства группы администрирования, для которой вы хотите изменить статусы устройств, одним из следующих способов:
   - Выберите имя группы администрирования.
   - Нажмите на кнопку **Показать иерархию** в верхней части страницы. В открывшейся панели наведите курсор мыши на название нужной группы и нажмите на значок параметров (⚙).

   Откроется окно свойств группы администрирования.
3. В окне свойств выберите вкладку **Статус устройства**.
4. Выберите раздел **Критический**.
5. В блоке **Установить статус "Критический", если** включите условие, чтобы перевести устройство в состояние *Критическое*.



Вы можете изменить только параметры, которые не заблокированы в родительской политике.

6. Установите переключатель рядом с условием в списке.
7. Нажмите на кнопку **Изменить** в верхнем левом углу списка.

8. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.

9. Нажмите на кнопку **OK**.

10. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

При выполнении заданных условий управляемому устройству присваивается статус *Критический*.

Чтобы изменить статус устройства на Предупреждение:

1. В главном окне приложения перейдите в раздел **Управление активами → Иерархия групп**.

2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.

3. В отобразившемся окне свойств выберите вкладку **Статус устройства**.

4. Выберите раздел **Предупреждение**.

5. В блоке **Установить статус "Предупреждение", если**, включите условие, чтобы переключить устройство в состояние *Предупреждение*.

   Вы можете изменить только параметры, которые не заблокированы в родительской политике.

6. Установите переключатель рядом с условием в списке.

7. Нажмите на кнопку **Изменить** в верхнем левом углу списка.

8. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.

9. Нажмите на кнопку **OK**.

10. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

При выполнении заданных условий управляемому устройству присваивается статус *Предупреждение*.

Смена Сервера администрирования для клиентских устройств

Вы можете сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером с помощью задачи **Смена Сервера администрирования**. После завершения задачи выбранные клиентские устройства будут под управлением указанного Сервера администрирования. Вы можете переключать управление устройством между следующими Серверами администрирования:

- главным Сервер администрирования и одним из его виртуальных Серверов администрирования;
- двумя виртуальными Серверами администрирования одного и того же главного Сервера администрирования.

Чтобы сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером:

1. В главном окне приложения перейдите в раздел **Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Параметры новой задачи** укажите следующие параметры:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky SIEM Cloud**.

   b. В поле **Тип задачи** выберите **Смена Сервера администрирования**.

   c. В поле **Название задачи** укажите название создаваемой задачи.

      Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

   d. Выберите устройства, которым будет назначена задача:

      - **Назначить задачу группе администрирования**

        Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

        Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

        Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, так как групповые задачи подчиняются параметрам групп безопасности, к которым они относятся.

      - **Задать адреса устройств вручную или импортировать из списка**

        Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

        Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

      - **Назначить задачу выборке устройств**

        Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

        Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

4. На шаге **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

5. На следующем шаге подтвердите свое согласие с условиями смены Сервера администрирования для клиентских устройств.

6. На следующем шаге выберите виртуальный Сервер администрирования, который вы хотите использовать для управления выбранными устройствами.

7. На шаге **Выбор учетной записи для запуска задачи** укажите параметры учетной записи:

   - **Учетная запись по умолчанию**

     Задача будет запускаться под той же учетной записью, под которой было установлено и запущено приложение, выполняющее эту задачу.

     По умолчанию выбран этот вариант.

   - **Задать учетную запись**

     В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

     - **Учетная запись**

       Учетная запись, от имени которой будет запускаться задача.

     - **Пароль**

       Пароль учетной записи, от имени которой будет запускаться задача.

8. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи.

   Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

9. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.

10. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

11. В окне свойств задачи укажите общие параметры задачи в соответствии с вашими требованиями.

12. Нажмите на кнопку **Сохранить**.

    Задача создана и настроена.

13. Запустите созданную задачу.

После завершения работы задачи клиентские устройства, для которых она была создана, переходят под управление Сервера администрирования, указанного в параметрах задачи.

Избегание конфликтов между Серверами администрирования

Если в сети имеется несколько Серверов администрирования, они могут видеть одни и те же клиентские устройства. Это может привести к тому, что, например, Сервер администрирования установит приложение, которое уже было установлено другим Сервером, а также к другим конфликтам. Чтобы запретить установку приложения на устройство, управляемое другим Сервером администрирования, нужно включить параметр **Устанавливать на устройства, управляемые только этим Сервером администрирования** в свойствах задачи *Удаленная установка приложения*.

Если вы включите параметр **Устанавливать на устройства, управляемые только этим Сервером администрирования** и запустите задачу *Удаленная установка приложения*, выполнится проверка для определения, находятся ли устройства под управлением другого Сервера администрирования. Для устройств, управляемых другим Сервером администрирования, для атрибута **Под управлением другого Сервера администрирования** будет установлено значение `true`. Задача *Удаленная установка приложения* к этим устройствам не применяется.

Значения атрибута **Под управлением другого Сервера администрирования** отображаются в столбце **Под управлением другого Сервера администрирования** в списке управляемых устройств и в списке нераспределенных устройств.

Свойство **Под управлением другого Сервера администрирования** можно также использовать как критерий для следующих операций:

- Отображение управляемых устройств.
- Выборки устройств.
- Правила перемещения устройств.
- Правила автоматического назначения тегов.

Чтобы сбросить атрибут Под управлением другого Сервера администрирования:

1. В главном меню OSMP Console перейдите в раздел **Управление активами** → **Нераспределенные устройства**.
2. Выберите нужное устройство и нажмите на кнопку **Удалить атрибут "Управляется другим Сервером администрирования"**.

Атрибут **Под управлением другого Сервера администрирования** будет сброшен.

Создание профилей подключения к Серверу администрирования

Чтобы автономные пользователи могли изменять способ подключения Агента администрирования к Серверу администрирования, необходимо настроить профили подключения к Серверу администрирования.

Чтобы создать профиль соединения:

1. В главном окне приложения перейдите в раздел **Управление активами** и выполните одно из следующих действий:
   - Если вы хотите создать профиль соединения для группы управляемых устройств, перейдите в раздел **Политики** и нажмите на **Агент администрирования Kaspersky Security Center**.
   - Если вы хотите создать профиль соединения для определенного управляемого устройства, перейдите в раздел **Управляемые устройства** и нажмите на имя устройства. В открывшемся окне перейдите на вкладку **Приложения** и нажмите на кнопку **Агент администрирования Kaspersky Security Center**.

   Откроется окно свойств политики Агента администрирования.
2. Перейдите на вкладку **Параметры приложения**, а затем перейдите в раздел **Подключения**.
3. В разделе **Профили соединений** нажмите на кнопку **Параметры**.

В разделе **Профили подключения к Серверу администрирования** отображается таблица профилей соединения.

Вы не можете просматривать, изменять или удалять профили соединения **Домашний Сервер администрирования** и **Офлайн-режим**.

4. Нажмите на кнопку **Добавить** и открывшемся окне укажите имя профиля.

Имя должно быть уникальным. Вы не можете использовать одно и то же имя для нескольких профилей.

5. При необходимости установите флажки в следующих полях:

- **Включить автономный режим, когда Сервер администрирования недоступен**.
- **Использовать прокси-сервер**.

  Если вы выбрали этот параметр:

  - Укажите информацию в полях **Адрес** и **Номер порта**.
  - При необходимости установите флажок **Аутентификация на прокси-сервере** и укажите имя пользователя и пароль в соответствующих полях.

6. Нажмите на кнопку **Сохранить**.

Новый профиль отобразится в таблице профилей соединения. Вы можете использовать его при настройке параметров **Сетевого месторасположения**.

Параметры сетевого местоположения определяют характеристики сети, к которой подключено клиентское устройство, и задают правила переключения Агента администрирования с одного профиля подключения Сервера администрирования на другой при изменении характеристик сети.

Вы можете изменять и удалять профили соединения.

Чтобы изменить профиль соединения:

1. В таблице профилей подключения нажмите на имя профиля соединения, который вы хотите изменить.
2. Внесите все необходимые изменения и нажмите на кнопку **Сохранить**.

Изменения применены к профилю соединения.

Чтобы удалить профиль соединения:

1. В таблице профилей соединения установите флажки рядом с профилями соединения, которые вы хотите удалить.
2. Нажмите на кнопку **Удалить**.

Выбранные профили соединения будут удалены.

О кластерах и массивах серверов

Kaspersky SIEM Cloud поддерживает кластерную технологию. Если Агент администрирования передает Серверу администрирования информацию о том, что приложение, установленное на клиентском устройстве, является частью массива сервера, то клиентское устройство становится узлом кластера.

Если группа администрирования содержит кластеры или массивы серверов, на странице **Управляемые устройства** отображаются две вкладки: одна для отдельных устройств, другая для кластеров и массивов серверов. После обнаружения управляемых устройств в качестве узлов кластера, кластер добавляется как отдельный объект на вкладку **Кластеры и массивы серверов**.

Узлы кластера или массивы серверов перечислены на вкладке **Устройства** вместе с другими управляемыми устройствами. Вы можете просматривать свойства узлов как отдельных устройств и выполнять другие операции, но удалить узел кластера или переместить его в другую группу администрирования отдельно от его кластера невозможно. Вы можете удалить или переместить только весь кластер.

Вы можете выполнять следующие операции с кластерами или массивами серверов:

- Посмотреть свойства.
- Переместить кластер или массив серверов в другую группу администрирования.

  При перемещении кластера или массива серверов в другую группу, все его узлы перемещаются вместе с ним, так как кластер и любой из его узлов всегда принадлежат к одной группе администрирования.
- Удалить.

  Целесообразно удалять кластер или массив серверов только тогда, когда кластер или массив серверов больше не существует в сети организации. Если кластер по-прежнему виден в вашей сети, а Агент администрирования и приложение "Лаборатории Касперского" по-прежнему установлено на узлах кластера, Open Single Management Platform автоматически возвращает удаленный кластер и его узлы обратно в список управляемых устройств.

Свойства кластеров или массивов серверов

Чтобы просмотреть параметры кластера или массива серверов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства** → **Кластеры и массивы серверов**.

   Отображается список кластеров и массивов серверов.

2. Нажмите на имя нужного кластера или массива серверов.

Откроется окно свойств выбранного кластера или массива серверов.

Общие

Раздел **Общие** отображает общую информацию о кластере или массиве серверов. Информация предоставляется на основании данных, полученных в ходе последней синхронизации узлов кластера с Сервером администрирования:

Имя

Описание

Windows-домен

Windows-домен или рабочая группа, содержащая кластер или массив серверов.

NetBIOS-имя

Имя кластера или массива серверов в сети Windows.

DNS-имя

Имя DNS-домена кластера или массива серверов.

Задачи

На вкладке **Задачи** вы можете управлять задачами, назначенными для кластеров и массивов серверов: просматривать список существующих задач, создавать новые, удалять, запускать и останавливать задачи, изменять параметры задач и просматривать результаты выполнения. Перечисленные задачи относятся к приложению безопасности "Лаборатории Касперского", установленного на узлах кластера. Open Single Management Platform получает список задач и информацию о статусе задач от узлов кластера. В случае отсутствия связи статус не отображается.

Узлы

На этой вкладке отображается список узлов, входящих в кластер или массив серверов. Вы можете нажать на имя узла, чтобы просмотреть окно свойств устройства.

Приложения "Лаборатории Касперского"

Окно свойств также может содержать дополнительные вкладки с информацией и параметрами, относящимися к приложению безопасности "Лаборатории Касперского", установленному на узлах кластера.

Теги устройств

Open Single Management Platform позволяет назначать теги устройствам. *Тег* представляет собой идентификатор устройства, который можно использовать для группировки, описания, поиска устройств. Назначенные устройствам теги можно использовать при создании выборок устройств, при поиске устройств и при распределении устройств по группам администрирования.

Теги могут назначаться устройствам вручную или автоматически. Теги можно назначать вручную, если требуется отметить отдельные устройства. Автоматическое назначение тегов выполняется Open Single Management Platform в соответствии с заданными правилами назначения тегов.

Автоматическое назначение тегов устройствам происходит при выполнении определенных правил. Каждому тегу соответствует отдельное правило. Правила могут применяться к сетевым свойствам устройства, операционной системе, установленным на устройстве приложениям и другим свойствам устройства. Например, если в вашей сети есть устройства под управлением Windows, Linux и macOS, вы можете настроить правило, которое будет назначать тег `[Linux]` всем устройствам с операционной системой Linux. Затем можно использовать этот тег при создании выборки устройств, чтобы отобрать все устройства с операционной системой Linux и назначить им задачу.

Вы можете добавить только одно правило автоматического назначения тегов для каждого тега. Если вы создадите еще одно правило для того же тега, предыдущее правило будет заменено.

Тег автоматически удаляется с устройства в следующих случаях:

- Устройство перестает удовлетворять условиям правила назначения тега.
- Правило назначения тега выключено или удалено.

Списки тегов и списки правил для каждого Сервера администрирования являются независимыми для всех Серверов администрирования, включая главный Сервер администрирования и подчиненные виртуальные Серверы администрирования. Правило применяется только к устройствам под управлением того Сервера администрирования, на котором оно создано.

Создание тегов устройств

Чтобы создать тег устройства:

1. В главном окне приложения перейдите в раздел **Хранилища → Теги устройств**.
2. Нажмите на кнопку **Добавить**.

   Отобразится окно создания тега.
3. В поле **Тег** введите название тега.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Новый созданный тег появляется в списке тегов устройства.

Изменение тегов устройств

Чтобы переименовать тег устройства:

1. В главном окне приложения перейдите в раздел **Хранилища → Теги устройств**.
2. Выделите тег, который требуется переименовать.

   Откроется окно свойств тега.
3. В поле **Тег** измените название тега.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Обновленный тег появится в списке тегов устройства.

Удаление тегов устройств

Чтобы удалить тег устройства:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Теги устройств**.
2. В списке выберите теги устройства, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.
4. В открывшемся окне нажмите на кнопку **Да**.

Выбранный тег устройства удален. Удаленный тег автоматически снимается со всех устройств, которым он был назначен.

Тег, который вы удалили, не удаляется автоматически из правил автоматического назначения тегов. После удаления тега он будет назначен новому устройству только при первом совпадении параметров устройства с условиями правила назначения тегов.

Удаленный тег не удаляется автоматически с устройства, если этот тег назначен устройству приложением или Агентом администрирования. Для того чтобы управлять такими тегами, используйте утилиту klscflag.

Просмотр устройств, которым назначен тег

Чтобы просмотреть устройства с назначенными тегами:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Теги устройств**.
2. Перейдите по ссылке **Просмотреть устройства** рядом с названием тега, для которого вы хотите посмотреть список назначенных устройств.

   Вы будете перенаправлены в раздел **Управляемые устройства** главного меню с устройствами, отфильтрованными по тегу, для которого вы нажали ссылку **Просмотреть устройства**.
3. Если вы хотите вернуться к списку тегов устройства, нажмите на кнопку **Назад** в браузере.

После просмотра устройств, которым назначен тег, вы можете создать и назначить новый тег или назначить существующий тег другим устройствам. В этом случае вам придется удалить фильтр по тегу, выбрать устройства и назначить тег.

Просмотр тегов, назначенных устройству

Чтобы просмотреть теги, назначенные устройству:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
2. Выберите устройство, теги которого требуется просмотреть.
3. В открывшемся окне свойств устройства выберите вкладку **Теги**.

   Отобразится список тегов, назначенных выбранному устройству. В столбце **Назначенный тег** вы можете просмотреть, как был назначен тег.

В панели инструментов можно выполнить следующие действия:

- Назначить устройству другой тег.
- Удалить уже назначенный тег.
- Просмотреть все теги устройств, которые существуют на Сервере администрирования.

Вы не можете просматривать назначенные теги локально на устройстве.

Назначение тегов устройствам вручную

Чтобы назначить тег устройству:

1. Просмотрите теги, уже назначенные устройству, которому вы ходите назначить тег.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне выполните одно из следующих действий:
   - Чтобы создать и добавить новый тег, выберите пункт **Создать тег** и укажите имя тега.
   - Чтобы выбрать существующий тег, выберите пункт **Назначить существующий тег** и в раскрывающемся списке выберите нужный тег.
4. Нажмите на кнопку **OK**, чтобы применить изменения.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   Выбранный тег будет назначен устройству.

Чтобы назначить тег нескольким устройствам:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
2. Выберите устройства, которым вы хотите назначить тег.

3. Нажмите на **Теги** и выберите пункт **Назначить** из раскрывающегося списка.

4. В открывшемся окне выберите тег из раскрывающегося списка.

   При необходимости можно выбрать несколько тегов.

   Также можно выполнить следующее:

   - Изменить тег, нажав на значок **Изменить** ( ).

     Укажите новое имя тега и нажмите на кнопку **Сохранить**.

     > Обратите внимание, что тег также будет переименован в списке тегов устройства.

   - Удалить тег, нажав на значок **Удалить** ( ).

     В появившемся окне нажмите на кнопку **Удалить**.

     > Обратите внимание, что тег также будет удален с Сервера администрирования.

5. Нажмите на кнопку **Сохранить**.

Теги назначены выбранным устройствам. Вы можете удалить назначенные теги.

Снятие назначенных тегов с устройств

> Снятый с устройства тег не удаляется. При необходимости его можно удалить вручную.

> Вы не можете вручную удалить теги, назначенные устройству приложениями или Агентом администрирования. Для того чтобы управлять этими тегами, используйте утилиту klscflag.

Чтобы снять назначенный тег с устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.

2. Выберите устройство, теги которого требуется просмотреть.

3. В открывшемся окне свойств устройства выберите вкладку **Теги**.

4. Установите флажок напротив тега, который требуется снять.

5. В верхней части списка нажмите на кнопку **Отменить назначение тега**.

6. В появившемся окне нажмите на кнопку **Да**.

Тег будет снят с устройства.

Чтобы удалить теги с нескольких устройств:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
2. Выберите устройства, теги которых вы хотите удалить.
3. Нажмите на **Теги** и в раскрывающемся списке выберите пункт **Отменить назначение**.
4. В открывшемся окне установите флажки рядом с тегами, которые вы хотите удалить.

   В окне отображаются все теги, назначенные всем устройствам, которые вы выбрали на шаге 2.

5. Нажмите на кнопку **Сохранить**.

Теги будут сняты с устройств.

Просмотр правил автоматического назначения тегов устройствам

Чтобы просмотреть правила автоматического назначения тегов устройствам,

Выполните одно из следующих действий:

- В главном окне приложения перейдите в раздел **Хранилища** → **Теги устройств** → **Правила автоматического назначения тегов**.
- Перейдите к просмотру тегов, назначенных устройству, а затем нажмите на кнопку **Настроить правила автоматического назначения тегов**.

Отобразится список правил автоматического назначения тегов устройствам.

Изменение правил автоматического назначения тегов устройствам

Чтобы изменить правило автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.
2. Выберите правило, которое требуется изменить.

   Откроется окно с параметрами правила.

3. Измените основные параметры правила:

   a. В поле **Имя правила** измените название правила.

      Название может содержать не более 256 символов.

   b. Выполните одно из следующих действий:

      - Включите правило, установив переключатель в положение **Правило включено**.
      - Выключите правило, установив переключатель в положение **Правило выключено**.

4. Выполните одно из следующих действий:

   - Если вы хотите добавить новое условие, нажмите на кнопку **Добавить** и в открывшемся окне укажите параметры нового условия.
   - Если вы хотите изменить существующее условие, выделите условие, которое требуется изменить, и измените его параметры.
   - Если вы хотите удалить условие, установите флажок рядом с именем условия, которое требуется удалить, и нажмите на кнопку **Удалить**.

5. В окне с параметрами условий нажмите на кнопку **OK**.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененное правило отображается в списке.

Создание правил автоматического назначения тегов устройствам

Чтобы создать правило автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.

2. Нажмите на кнопку **Добавить**.

   Откроется окно с параметрами нового правила.

3. Укажите основные параметры правила:

   a. В поле **Имя правила** введите название правила.

      Название может содержать не более 256 символов.

   b. Выполните одно из следующих действий:

      - Включите правило, установив переключатель в положение **Правило включено**.
      - Выключите правило, установив переключатель в положение **Правило выключено**.

   c. В поле **Тег** укажите новое название тега устройства или выберите существующий тег устройства из списка.

      Название может содержать не более 256 символов.

4. В поле выбора условия нажмите на кнопку **Добавить**, чтобы добавить новое условие.

   Откроется окно с параметрами нового условия.

5. Укажите название условия.

   Название может содержать не более 256 символов. Название условия должно быть уникальным в рамках одного правила.

6. Настройте срабатывание правила по следующим условиям: Можно выбрать несколько условий.

   - **Сеть** – сетевые свойства устройства (например, имя устройства в сети Windows, принадлежность устройства к домену или к IP-подсети).

     Если для базы данных, которую вы используете для Open Single Management Platform, настроена сортировка с учетом регистра, учитывайте регистр при указании DNS-имени устройства. Иначе правила автоматического назначения тегов не будет работать.

   - **Приложения** – наличие на устройстве Агента администрирования, тип, версия, архитектура операционной системы и менеджер пакетов.
   - **Виртуальные машины** – принадлежность устройства к определенному типу виртуальных машин.
   - **Active Directory** – нахождение устройства в подразделении Active Directory и членство устройства в группе Active Directory.
   - **Реестр приложений** – наличие на устройстве приложений различных производителей.

7. Нажмите на кнопку **OK**, чтобы сохранить изменения.

   При необходимости можно задать несколько условий для одного правила. В этом случае тег будет назначен устройствам, если для них выполняется хотя бы одно из условий.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Созданное правило выполняется на устройствах, управляемых выбранным Сервером администрирования. Если параметры устройства соответствуют условиям правила, этому устройству назначается тег.

В дальнейшем правило применяется в следующих случаях:

- Автоматически, регулярно, в зависимости от загрузки сервера.
- После изменения правила.
- После выполнения правила вручную.
- После того как Сервер администрирования обнаружит изменения, которые соответствуют условиям правила, в параметрах устройства или в параметрах группы, которая содержит это устройство.

Вы можете создать несколько правил назначения тегов. Одному устройству может быть назначено несколько тегов, в случае если вы создали несколько правил назначения тегов и условия этих правил выполняются одновременно. Вы можете просмотреть список всех назначенных тегов в свойствах устройства.

Выполнение правил автоматического назначения тегов устройствам

Когда выполняется правило, тег, указанный в свойствах этого правила, назначается устройству, которое соответствует условиям, указанным в свойствах правила. Можно выполнять только активные правила.

Чтобы выполнить правила автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.
2. Установите флажки напротив активных правил, которые требуется выполнить.
3. Нажмите на кнопку **Выполнить правило**.

Выбранные правила будут выполнены.

Удаление правил автоматического назначения тегов с устройств

Чтобы удалить правило автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.
2. Установите флажок напротив правила, которое требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**.

Выбранное правило будет удалено. Тег, указанный в свойствах этого правила, будет снят со всех устройств, которым он был назначен.

Снятый с устройства тег не удаляется. При необходимости его можно удалить вручную.

Управление тегами устройств с помощью утилиты klscflag

Чтобы назначить набор тегов устройству, вам нужно запустить утилиту klscflag на клиентском устройстве, которому вы хотите назначить теги.

Утилита klscflag перезаписывает существующие теги, назначенные устройству. Это означает, что вы можете добавить или удалить теги, указав нужный набор тегов в команде. Утилита не имеет команд для добавления или удаления отдельных тегов. Вы изменяете весь набор тегов.

При указании тегов в командах, таких как klscflag, рекомендуется использовать символы одного регистра, например все буквы заглавные. Использование всех заглавных букв поможет избежать возможных проблем с тегами, которые отличаются только регистром, в зависимости от конфигурации СУБД.

Чтобы назначить один или несколько тегов вашему устройству с помощью утилиты klscflag:

1. Запустите командную строку под учетной записью с правами root и измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в директории установки Агента администрирования. По умолчанию директория установки – /opt/kaspersky/ksc64/sbin.
2. Введите одну из следующих команд:
   - Чтобы назначить набор тегов:

```
/opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"TAG 1\",\"TAG 2\",\"TAG 3\"]" -
svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
```

где `[\"TAG 1\",\"TAG 2\",\"TAG 3\"]` это список тегов, которые вы хотите назначить устройству.

Если вы оставите квадратные скобки пустыми, это удалит все теги с устройства:

```
/opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type =
\"SS_PRODINFO\";"
```

- Чтобы назначить новый тег существующему набору тегов:

  ```
  /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
  KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NEW TAG\",\"TAG 1\",\"TAG
  2\",\"TAG 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
  ```

  где `NEW TAG` – это тег, который вы хотите назначить устройству, `TAG 1`, `TAG 2`, `TAG 3` – это теги, которые уже назначены устройству.

- Чтобы удалить определенный тег, не удаляя другие теги, уже назначенные устройству, выполните команду с обновленным набором тегов.

  Например, если `TAG 1`, `TAG 2`, `TAG 3` – ваши текущие теги и вы хотите удалить `TAG 2`, выполните следующую команду:

  ```
  /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
  KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"TAG 1\",\"TAG 3\"]" -svt ARRAY_T
  -ss "|ss_type = \"SS_PRODINFO\";"
  ```

3. Перезапустите службу Агента администрирования.

   Утилита klscflag назначит вашему устройству указанные теги.

4. Если вы хотите убедиться, что утилита klscflag успешно назначила указанные теги, просмотрите теги, которые были назначены устройству.

Также можно назначать теги устройств вручную.

Карантин и Файлы резервного хранилища

Приложения защиты "Лаборатории Касперского", установленные на клиентских устройствах, в процессе проверки устройств могут помещать файлы в раздел Карантин или в раздел Файлы резервного хранилища.

Карантин – это специальное хранилище, в которое помещаются файлы, возможно зараженные вирусами или неизлечимые на момент обнаружения.

Файлы резервного хранилища предназначены для хранения резервных копий файлов, которые были удалены или изменены в процессе лечения.

Kaspersky SIEM Cloud формирует общий список файлов, помещенных в раздел Карантин или в раздел Файлы резервного хранилища приложениями "Лаборатории Касперского" на устройствах. Агенты администрирования клиентских устройств передают информацию о файлах в разделе Карантин или в разделе Файлы резервного хранилища на Сервер администрирования.

Kaspersky SIEM Cloud не копирует файлы из хранилищ на Сервер администрирования. Все файлы размещаются в хранилищах на устройствах.

Загрузка файла из хранилища

Kaspersky SIEM Cloud позволяет загружать копии файлов, помещенных приложением безопасности в раздел Карантин или в раздел Файлы резервных копий на клиентском устройстве. Файлы копируются в указанную вами папку.

Вы можете загружать файлы только если выполняется одно из двух условий: либо параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, либо используется шлюз соединения. Иначе загрузка невозможна.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

Чтобы сохранить копию файла из раздела Карантин или Файлы резервных копий на жесткий диск:

1. Выполните одно из следующих действий:

   - Если вы хотите сохранить копию файла из Карантина, в главном меню перейдите в раздел **Хранилища → Карантин**.

   - Если вы хотите сохранить копию файла из Файлы резервных копий, в главном меню перейдите в раздел **Хранилища → Файлы резервных копий**.

2. В открывшемся окне выберите файл, который вы хотите загрузить, и нажмите **Скачать**.

   Начнется загрузка. Копия файла, помещенного в Карантин на клиентском устройстве, сохраняется в указанную папку.

Удаление файлов из хранилища

Чтобы удалить файл, помещенный в раздел Карантин или в раздел Файлы резервных копий:

1. В главном окне приложения перейдите в раздел **Операции → Хранилища** и выберите один из следующих разделов:

   - **Карантин**, если вы хотите удалить файл из карантина.

   - **Файлы резервных копий**, если вы хотите удалить файл из резервного хранилища.

2. В зависимости от выбранного хранилища выполните одно из следующих действий:

   - В разделе **Файлы резервных копий** выберите файл из списка и нажмите на кнопку **Удалить**.
   - В разделе **Карантин** удалите файл одним из следующих способов:
     - Установите флажок рядом с именем файла, который нужно удалить, а затем в панели инструментов нажмите на кнопку **Удалить**.
     - Нажмите на имя файла, который нужно удалить, и в открывшемся окне свойств в панели инструментов нажмите на кнопку **Удалить**.

       В этом случае файл будет удален, на экране отобразится соответствующее уведомление, окно со свойствами закроется.

Приложение безопасности на клиентском устройстве, которое поместило файлы в хранилище (Карантин или Файлы резервных копий), удаляет файлы из этого хранилища.

Удаленная диагностика клиентских устройств

Вы можете использовать удаленную диагностику для удаленного выполнения следующих операций на клиентских устройствах на базе Windows и на базе Linux:

- включения и выключения трассировки, изменения уровня трассировки и загрузки файла трассировки;
- загрузки системной информации и параметров приложения;
- загрузки журналов событий;
- создание файла дампа для приложения;
- запуска диагностики и загрузки результатов диагностики;
- запуск, остановка и перезапуск приложений.

Вы можете использовать журнал событий и диагностические отчеты, загруженные с клиентского устройства, для устранения неполадок самостоятельно. Также если вы обращаетесь в Службу технической поддержки "Лаборатории Касперского", эксперт технической поддержки "Лаборатории Касперского" может попросить вас загрузить файлы трассировки, файлы дампа, журнал событий и диагностические отчеты с клиентского устройства для дальнейшего анализа в "Лаборатории Касперского".

Открытие окна удаленной диагностики

Чтобы выполнить удаленную диагностику клиентских устройств на базе Windows и на базе Linux, сначала нужно открыть окно удаленной диагностики.

Чтобы открыть окно удаленной диагностики:

1. Чтобы выбрать устройство, для которого вы хотите открыть окно удаленной диагностики, выполните одно из следующих действий:

   - Если устройство принадлежит к группе администрирования, в главном меню перейдите в раздел **Управление активами** → **Управляемые устройства**.

   - Если устройство принадлежит к группе нераспределенных устройств, в главном меню перейдите в раздел **Управление активами** → **Нераспределенные устройства**.

2. Нажмите на имя требуемого устройства.

3. В открывшемся окне свойств устройства выберите вкладку **Дополнительно**.

4. На вкладке **Дополнительно** нажмите **Удаленная диагностика**.

   В результате открывается окно **Удаленная диагностика** клиентского устройства. Если отсутствует соединение между Сервером администрирования и клиентским устройством, появится сообщение об ошибке.

Если вам нужно получить сразу всю диагностическую информацию о клиентском устройстве с операционной системой Linux, вы можете запустить на этом устройстве скрипт collect.sh.

Включение и выключение трассировки для приложений

Вы можете включать и выключать трассировку для приложений, включая трассировку xperf.

Включение и выключение трассировки

Чтобы включить или выключить трассировку на удаленном устройстве:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В дереве объектов устройства выберите приложение, для которого требуется включить или выключить трассировку.

   Откроется список параметров удаленной диагностики.

4. Если вы хотите включить трассировку:

   a. В разделе **Трассировка** нажмите на кнопку **Включить трассировку**.

   b. В открывшемся окне **Изменить уровень трассировки** рекомендуется не менять значения, заданные по умолчанию. При необходимости эксперт Службы технической поддержки проведет вас через процесс настройки. Доступны следующие параметры:

      - **Уровень трассировки**

        Уровень трассировки определяет состав информации, которую содержит файл трассировки.

- **Трассировка на основе ротации**

  Приложение перезаписывает информацию трассировки, чтобы предотвратить чрезмерное увеличение файла трассировки. Укажите максимальное количество файлов, которые будут использоваться для хранения информации трассировки, и максимальный размер каждого файла. Если записано максимальное количество файлов трассировки максимального размера, самый старый файл трассировки будет удален, чтобы можно было записать новый файл трассировки.

  Этот параметр доступен только для Kaspersky Endpoint Security.

c. Нажмите на кнопку **Сохранить**.

Трассировка включена для выбранного приложения. В некоторых случаях для включения трассировки приложения безопасности требуется перезапустить это приложение и его задачу.

> На клиентских устройствах под управлением Linux трассировка компонента Обновление Kaspersky Security Agent регулируется параметрами Агента администрирования. Поэтому параметры **Включить трассировку** и **Изменить уровень трассировки** выключены для этого компонента на клиентских устройствах под управлением Linux.

5. Если вы хотите выключить трассировку для выбранного приложения, нажмите на кнопку **Выключить трассировку**.

   Трассировка выключена для выбранного приложения.

Включение трассировки Xperf

Для Kaspersky Endpoint Security эксперты Службы технической поддержки могут попросить вас включить трассировку Xperf для получения информации о производительности системы.

Чтобы включить, настроить или отключить трассировку Xperf:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В списке приложений выберите Kaspersky Endpoint Security для Windows.

   Откроется список параметров удаленной диагностики для Kaspersky Endpoint Security для Windows.

4. В разделе **Трассировка Xperf** нажмите на кнопку **Включить трассировку Xperf**.

   Если трассировка Xperf уже включена, отображается кнопка **Выключить трассировку Xperf**. Нажмите на эту кнопку, если хотите отключить трассировку Xperf для Kaspersky Endpoint Security для Windows.

5. В открывшемся окне **Изменить уровень трассировки Xperf**, в зависимости от запроса эксперта Службы технической поддержки, выполните следующее:

   a. Выберите один из уровней трассировки:

   - **Легкий уровень**

     Файл трассировки этого типа содержит минимальный объем информации о системе.

     По умолчанию выбран этот вариант.

- **Детальный уровень**

  Файл трассировки этого типа содержит более подробную информацию, чем файл типа *Легкий уровень*, и может запрашиваться специалистами Технической поддержки, если информации в файле трассировки *легкого уровня* недостаточно для оценки производительности. Файл трассировки *Детального уровня* содержит информацию об оборудовании, операционной системе, список запущенных и завершенных процессов и приложений, событиях, используемых для оценки производительности, а также события Средства оценки системы Windows.

b. Выберите один из уровней трассировки Xperf:

- **Базовый тип**

  Приложение получает данные трассировки во время работы приложения Kaspersky Endpoint Security.

  По умолчанию выбран этот вариант.

- **Тип перезагрузки**

  Приложение получает данные трассировки, когда на управляемом устройстве запускается операционная система. Этот тип трассировки эффективен, когда проблема, влияющая на производительность системы, возникает после включения устройства и перед запуском Kaspersky Endpoint Security.

Также вам могут предложить включить параметр **Размер файлов ротации (МБ)**, чтобы предотвратить чрезмерное увеличение файла трассировки. Затем укажите максимальный размер файла трассировки. Когда файл достигает максимального размера, самый старый файл трассировки будет перезаписан новым файлом.

c. Определите размер файла ротации.

d. Нажмите на кнопку **Сохранить**.

Трассировка Xperf включена и настроена.

6. Если вы хотите отключить трассировку Xperf для Kaspersky Endpoint Security для Windows, нажмите **Выключить трассировку Xperf** в разделе **Трассировка Xperf**.

   Трассировка Xperf выключена.

Загрузка файла трассировки приложения

Вы можете загрузить файлы трассировки с клиентского устройства только если выполняется одно из двух условий: либо параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, либо используется шлюз соединения. Иначе загрузка невозможна..

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

Чтобы загрузить файл трассировки приложения:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В списке приложений выберите приложение, для которого вы хотите загрузить файл трассировки.
4. В разделе **Трассировка** нажмите на кнопку **Файлы трассировки**.

   Откроется окно **Журналы удаленной установки**, где отображается список файлов трассировки.
5. В списке файлов трассировки выберите файл, который вы хотите загрузить.
6. Выполните одно из следующих действий:

   - Загрузите выбранный файл, нажав на кнопку **Скачать**. Вы можете выбрать один или несколько файлов для загрузки.
   - Загрузите часть выбранного файла:

     a. Нажмите на кнопку **Скачать часть**.

     Одновременная частичная загрузка нескольких файлов невозможна. Если вы выберете более одного файла трассировки, кнопка **Скачать часть** будет неактивна.

     b. В открывшемся окне укажите имя и часть файла для загрузки в соответствии с вашими требованиями.

     Для устройств под управлением Linux изменение имени части файла недоступно.

     c. Нажмите на кнопку **Скачать**.

Выбранный файл или его часть загружается в указанное вами расположение.

Удаление файлов трассировки

Вы можете удалить файлы трассировки, которые больше не нужны.

Чтобы удалить файл трассировки, выполните следующее действие:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В открывшемся окне удаленной диагностики выберите раздел **Журналы событий**.
3. В разделе **Файлы трассировки** нажмите **Журналы службы Центра обновления Windows** или **Журналы удаленной установки**, в зависимости от того, какие файлы трассировки вы хотите удалить.

   Откроется окно **Журналы удаленной установки**, где отображается список файлов трассировки.
4. В списке файлов трассировки выберите один или несколько файлов, которые вы хотите удалить.
5. Нажмите на кнопку **Удалить**.

Выбранные файлы трассировки удалены.

Загрузка параметров приложений

Вы можете загрузить параметры приложений с клиентского устройства только если выполняется одно из двух условий: либо параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, либо используется шлюз соединения. Иначе загрузка невозможна.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

Чтобы загрузить с клиентского устройства параметры программ:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.
3. В разделе **Параметры приложения** нажмите на кнопку **Скачать** для загрузки информации о параметрах приложений, установленных на клиентском устройстве.

ZIP-архив с информацией загрузится в указанное расположение.

Загрузка системной информации с клиентского устройства

Вы можете загрузить системную информацию с клиентского устройства на свое устройство только если выполняется одно из двух условий: либо параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, либо используется шлюз соединения. Иначе загрузка невозможна.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

Чтобы загрузить системную информацию с клиентского устройства выполните следующие действия:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Информация о системе**.
3. Нажмите на кнопку **Скачать** для загрузки системной информации о клиентском устройстве.

> Архив может содержать конфиденциальные данные (например, ключи и пароли) в виде обычного текста. Рекомендуется просмотреть файлы в архиве и удалить такие данные перед отправкой в Службу технической поддержки "Лаборатории Касперского".

Файл с информацией загрузится в указанное расположение.

Загрузка журналов событий

Вы можете загружать журналы событий с клиентского устройства на свое устройство только если выполняется одно из двух условий: либо параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, либо используется шлюз соединения. Иначе загрузка невозможна.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

Чтобы загрузить с удаленного устройства журнал событий:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В разделе **Журналы событий** в окне удаленной диагностики выберите **Все журналы устройства**.
3. В окне **Все журналы событий устройства** выберите один или несколько журналов событий.
4. Выполните одно из следующих действий:
   - Загрузите выбранный журнал событий, нажав на кнопку **Скачать весь файл**.
   - Загрузите часть выбранного журнала событий:
     a. Нажмите на кнопку **Скачать часть**.
     Одновременная частичная загрузка нескольких журналов событий невозможна. Если вы выберете более одного журнала событий, кнопка **Скачать часть** будет неактивна.
     b. В открывшемся окне укажите имя и часть журнала событий для загрузки в соответствии с вашими требованиями.
     c. Нажмите на кнопку **Скачать**.

Выбранный журнал событий или его часть загрузится в указанное расположение.

Запуск, остановка и перезапуск приложения

Вы можете запускать, останавливать и перезапускать приложения на клиентском устройстве.

Чтобы запустить, остановить или перезапустить приложение:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.
   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите приложение, которое вы хотите запустить, остановить или перезапустить.
4. Выберите действие, нажав на одну из следующих кнопок:
   - **Остановить приложение**
     Эта кнопка доступна, только если приложение в данный момент запущено.
   - **Перезапустить приложение**
     Эта кнопка доступна, только если приложение в данный момент запущено.
   - **Запустить приложение**
     Эта кнопка доступна, только если приложение в данный момент не запущено.

В зависимости от выбранного вами действия требуемое приложение запустится, остановится или перезапустится на клиентском устройстве.

Если вы перезапустите Агент администрирования, появится сообщение о том, что текущее соединение устройства с Сервером администрирования будет потеряно.

Запуск удаленной диагностики приложения и загрузка результатов

Чтобы запустить диагностику приложения на удаленном устройстве и загрузить ее результаты:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите приложение, для которого вы хотите запустить удаленную диагностику.

   Откроется список параметров удаленной диагностики.
4. В разделе **Отчет диагностики** нажмите на кнопку **Выполнить диагностику**.

   Запускается процесс удаленной диагностики и генерируется отчет о диагностике. После завершения процесса диагностики кнопка **Скачать отчет диагностики** становится доступной.
5. Нажмите на кнопку **Скачать отчет диагностики**, чтобы загрузить отчет.

Отчет загрузится в указанное расположение.

Запуск приложения на клиентском устройстве

Вам может потребоваться запустить приложение на клиентском устройстве, если вас об этом попросит специалист Службы технической поддержки "Лаборатории Касперского". Вам не нужно устанавливать приложение самостоятельно на этом устройстве.

Если вы хотите запустить пользовательский скрипт на клиентском устройстве, вы можете использовать переменную среды `KLACDT_SAVE_SETTING`, чтобы определить путь, по которому будут сохранены результаты выполнения. Например:

- Для устройств с операционной системой Windows:

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```

- Для устройств с операционной системой Linux:

  ```
  echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

Чтобы запустить приложение на клиентском устройстве:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Запуск удаленного приложения**.

3. В поле **Тип объекта** выберите тип объекта, который вы хотите загрузить:

   - Выберите **Файл** для загрузки исполняемого файла.
   - Выберите **Папка** для загрузки папки, содержащей приложение, которое вы хотите запустить на клиентском устройстве.

     Если вы выберете этот тип объекта, отобразится поле **Имя исполняемого файла, который будет запущен**. В этом поле укажите имя исполняемого файла в папке. Также можно указать относительный путь к файлу.
   - Выберите **Архив** для загрузки ZIP-архива, содержащего приложение, которое вы хотите запустить на клиентском устройстве.

     Если вы выберете этот тип объекта, отобразится поле **Имя исполняемого файла, который будет запущен**. В этом поле укажите имя исполняемого файла в папке, который вы хотите запустить на клиентском устройстве. Также можно указать относительный путь к файлу.

     > ZIP-архив должен содержать папку утилиты. Эта папка содержит исполняемый файл для запуска на удаленном устройстве.

4. Загрузите объект, выбрав его в системном окне или перетащив его в поле загрузки.
5. При необходимости в поле **Аргументы командной строки** укажите аргументы командной строки, которые будут переданы при запуске исполняемого файла.
6. Нажмите на кнопку **Загрузить и запустить** для запуска выбранного приложения на клиентском устройстве.
7. После успешного выполнения приложения, загрузите результаты выполнения, нажав на кнопку **Скачать результаты выполнения приложения**.

   > Результаты выполнения приложения хранятся до тех пор, пока вы не запустите новую диагностику или не закроете окно.

Удаленная диагностика клиентского устройства с использованием приложения завершена.

Создание файла дампа для приложения

Файл дампа приложения позволяет просматривать параметры приложения, работающего на клиентском устройстве, в определенный момент времени. Этот файл также содержит информацию о модулях, которые были загружены для приложения.

> Создание файлов дампа доступно только для 32-разрядных процессов, работающих на клиентских устройствах под управлением Windows. Для клиентских устройств под управлением Linux и для 64-битных процессов эта функция не поддерживается.

Чтобы создать файл дампа для приложения:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Запуск удаленного приложения**.

3. В разделе **Формирование файла дампа процесса** укажите исполняемый файл приложения, для которого вы хотите создать файл дампа.

4. Нажмите на кнопку **Скачать**, чтобы сохранить файл дампа указанного приложения.

   Если указанное приложение не запущено на клиентском устройстве, отобразится сообщение об ошибке.

Удаленное подключение к рабочему столу клиентского устройства

Вы можете получить удаленный доступ к рабочему столу клиентского устройства с помощью Агента администрирования, установленного на устройстве. Удаленное подключение к клиентскому устройству с помощью Агента администрирования возможно и в том случае, если TCP- и UDP-порты клиентского устройства закрыты для доступа.

После подключения к устройству вы получаете полный доступ к информации на этом устройстве и может управлять приложениями, установленными на нем.

Удаленное подключение должно быть разрешено в параметрах операционной системы целевого управляемого устройства. Например, в Windows 10 этот параметр называется **Разрешить подключения удаленного помощника к этому компьютеру** (его можно найти **Панель управления** → **Система и безопасность** → **Система** → **Настройка удаленного доступа**). Если у вас есть лицензия на Системное администрирование, вы можете принудительно включить этот параметр, когда установлено соединение с управляемым устройством. Если у вас нет лицензии, включите этот параметр локально на целевом управляемом устройстве. Если этот параметр выключен, удаленное подключение невозможно.

Чтобы установить удаленное соединение с устройством, у вас должно быть две утилиты:

- Утилита klsctunnel "Лаборатории Касперского". Эта утилита должна храниться на вашей рабочей станции. Вы используете эту утилиту для туннелирования соединения между клиентским устройством и Сервером администрирования.

  Kaspersky SIEM Cloud позволяет туннелировать TCP-соединения от Консоли администрирования через Сервер администрирования и далее через Агент администрирования к заданному порту на управляемом устройстве. Туннелирование используется для подключения клиентского приложения, находящегося на устройстве с установленной Консолью администрирования, к TCP-порту на управляемом устройстве, если прямое соединение устройства с Консолью администрирования с устройством невозможно.

  С помощью утилиты klsctunnel можно подключиться к устройствам только под управлением Windows и Linux.

  Туннелирование соединения удаленного клиентского устройства с Сервером администрирования необходимо, если на устройстве недоступен порт для соединения с Сервером администрирования. Порт на устройстве может быть недоступен в следующих случаях:

  - Удаленное устройство подключено к локальной сети, в которой используется механизм NAT.
  - Удаленное устройство входит в локальную сеть Сервера администрирования, но его порт закрыт сетевым экраном.

- Стандартный компонент Microsoft Windows "Подключение к удаленному рабочему столу". Подключение к удаленному рабочему столу выполняется с помощью штатной утилиты Windows mstsc.exe в соответствии с параметрами работы этой утилиты.

  Подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. Как только вы подключаетесь к сеансу, пользователь устройства автоматически отключается от сеанса; пользователь не получает предварительного уведомления.

Для подключения к рабочему столу клиентского устройства должно выполняться одно из следующий условий:

- Клиентское устройство является членом группы администрирования, которая имеет точку распространения с включенным параметром **Не разрывать соединение с Сервером администрирования**.

- В параметрах клиентского устройства включен параметр **Не разрывать соединение с Сервером администрирования**.

  Общее количество клиентских устройств с выбранным параметром **Не разрывать соединение с Сервером администрирования** не может превышать 300.

Чтобы удалено подключиться к рабочему столу клиентского устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.

2. Установите флажок напротив устройства, к которому вы хотите получить доступ.

3. Нажмите на кнопку **Подключиться к удаленному рабочему столу**.

   Откроется окно Подключиться к удаленному рабочему столу.

4. Нажмите на кнопку **Скачать**, чтобы загрузить утилиту klsctunnel.

5. Нажмите на кнопку **Копировать в буфер обмена**, чтобы скопировать текст из текстового поля. Этот текст представляет собой двоичный объект данных (BLOB), который содержит параметры, необходимые для установления соединения между Сервером администрирования и управляемым устройством.

   > Объект BLOB действителен в течение 3 минут. Если срок его действия истек, снова откройте окно Подключиться к удаленному рабочему столу, чтобы сгенерировать новый объект BLOB.

6. Запустите утилиту klsctunnel.

   Откроется окно утилиты.

7. Вставьте скопированный текст в текстовое поле.

8. Если вы используете прокси-сервер, установите флажок **Использовать прокси-сервер**, а затем укажите параметры подключения к прокси-серверу.

9. Нажмите на кнопку **Открыть порт**.

   Откроется окно входа в систему подключения к удаленному рабочему столу.

10. Укажите учетные данные учетной записи, под которой вы в настоящий момент входите OSMP Console.

11. Нажмите на кнопку **Подключиться**.

После подключения к клиентскому устройству рабочий стол клиентского устройства доступен в окне удаленного подключения Microsoft Windows.

Подключение к устройствам с помощью совместного доступа к рабочему столу Windows

Вы можете получить удаленный доступ к рабочему столу клиентского устройства с помощью Агента администрирования, установленного на устройстве. Удаленное подключение к клиентскому устройству с помощью Агента администрирования возможно и в том случае, если TCP- и UDP-порты клиентского устройства закрыты для доступа.

Вы можете подключиться к существующему сеансу на клиентском устройстве, не отключая пользователя, работающего в этом сеансе. В этом случае у вас и у пользователя сеанса на устройстве есть совместный доступ к рабочему столу.

Чтобы установить удаленное соединение с устройством, у вас должно быть две утилиты:

- Утилита klsctunnel "Лаборатории Касперского". Эта утилита должна храниться на вашей рабочей станции. Вы используете эту утилиту для туннелирования соединения между клиентским устройством и Сервером администрирования.

  Kaspersky SIEM Cloud позволяет туннелировать TCP-соединения от Консоли администрирования через Сервер администрирования и далее через Агент администрирования к заданному порту на управляемом устройстве. Туннелирование используется для подключения клиентского приложения, находящегося на устройстве с установленной Консолью администрирования, к TCP-порту на управляемом устройстве, если прямое соединение устройства с Консолью администрирования с устройством невозможно.

  Туннелирование соединения удаленного клиентского устройства с Сервером администрирования необходимо, если на устройстве недоступен порт для соединения с Сервером администрирования. Порт на устройстве может быть недоступен в следующих случаях:

  - Удаленное устройство подключено к локальной сети, в которой используется механизм NAT.
  - Удаленное устройство входит в локальную сеть Сервера администрирования, но его порт закрыт сетевым экраном.

- Совместный доступ к рабочему столу Windows. При подключении к существующему сеансу удаленного рабочего стола пользователь этого сеанса на устройстве получит от вас запрос на подключение. Информация о процессе удаленной работы с устройством и результатах этой работы не сохраняется в отчетах Kaspersky SIEM Cloud.

  Вы можете настроить аудит действий на удаленном клиентском устройстве. В ходе аудита приложение сохраняет информацию о файлах на клиентском устройстве, которые открывал и/или изменял администратор.

Для подключения к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows требуется выполнение следующих условий:

- На вашей рабочей станции установлена операционная система Microsoft Windows Vista или более поздняя версия.

  Чтобы проверить, включена ли функция совместного доступа к рабочему столу Windows в вашей версии Windows, убедитесь, что ключ CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} включен в 32-разрядный реестр.

- На клиентском устройстве установлена операционная система Microsoft Windows Vista или более поздняя версия.
- Kaspersky SIEM Cloud использует лицензию на управление уязвимостями и исправлениями.
- Клиентское устройство является членом группы администрирования, которая имеет точку распространения с включенным параметром **Не разрывать соединение с Сервером администрирования**, или этот параметр включен в свойствах клиентского устройства.

  Обратите внимание, что общее количество клиентских устройств с включенным параметром **Не разрывать соединение с Сервером администрирования** не может превышать 300.

Чтобы подключиться к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows:

1. В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства**.
2. Установите флажок напротив устройства, к которому вы хотите получить доступ.
3. Нажмите на кнопку **Совместный доступ к рабочему столу Windows**.

   Открывается мастер Совместный доступ к рабочему столу Windows.
4. Нажмите на кнопку **Скачать**, чтобы загрузить утилиту klsctunnel, и дождитесь завершения процесса загрузки.

   Если у вас уже есть утилита klsctunnel, пропустите этот шаг.
5. Нажмите на кнопку **Далее**.
6. Выберите сеанс на устройстве, к которому вы хотите подключиться, а затем нажмите на кнопку **Далее**.
7. На целевом устройстве в открывшемся окне пользователь должен разрешить сеанс совместного доступа к рабочему столу. Иначе сеанс невозможен.

   После того как пользователь подтвердит сеанс совместного доступа к рабочему столу, мастер откроет следующий шаг.
8. Нажмите на кнопку **Копировать в буфер обмена**, чтобы скопировать текст из текстового поля. Этот текст представляет собой двоичный объект данных (BLOB), который содержит параметры, необходимые для установления соединения между Сервером администрирования и управляемым устройством.

   > Объект BLOB действителен в течение 3 минут. Если срок его действия истек, сгенерируйте объект BLOB.
9. Запустите утилиту klsctunnel.

   Откроется окно утилиты.
10. Вставьте скопированный текст в текстовое поле.
11. Если вы используете прокси-сервер, установите флажок **Использовать прокси-сервер**, а затем укажите параметры подключения к прокси-серверу.
12. Нажмите на кнопку **Открыть порт**.

Совместный доступ к рабочему столу запускается в новом окне. Если вы хотите взаимодействовать с устройством, нажмите на значок меню ( ) в верхнем левом углу окна и выберите **Интерактивный режим**.

Срабатывание правил в режиме Интеллектуального обучения

В этом разделе представлена информация об обнаружениях, выполненных правилами Адаптивного контроля аномалий Kaspersky Endpoint Security для Windows на клиентских устройствах.

Правила обнаруживают аномальное поведение на клиентских устройствах и могут блокировать его. Если правила работают в режиме Интеллектуального обучения, они обнаруживают аномальное поведение и отправляют отчеты о каждом таком случае на Сервер администрирования Kaspersky SIEM Cloud. Вы можете просмотреть отчеты об анализе аномального поведения в разделе **Хранилища → Правила срабатываний в статусе Интеллектуальное обучение**. Вы можете подтвердить обнаружение как корректное или добавить его в исключения, после чего такой тип поведения не будет считаться аномальным.

Информация об обнаружениях хранится в журнале событий на Сервере администрирования (вместе с остальными событиями) и в отчете Адаптивный контроль аномалий.

Подробная информация об Адаптивном контроле аномалий, его правилах, их режимах и статусах приведена в справке Kaspersky Endpoint Security.

Просмотр списка обнаружений, выполненных с помощью правил Адаптивного контроля аномалий

Чтобы просмотреть список обнаружений, выполненных с помощью правил Адаптивного контроля аномалий:

1. В главном окне приложения перейдите в раздел **Хранилища → Правила срабатываний в статусе Интеллектуальное обучение**.

   В списке отображается следующая информация об обнаружении, выполняемая с помощью правил Адаптивного контроля аномалий:

   - **Группа администрирования**

     Имя группы администрирования, в которую включено устройство.

   - **Имя устройства**

     Имя клиентского устройства, на котором было применено правило.

   - **Имя**

     Имя правила, которое было применено.

   - **Статус**

     Исключение – если администратор обработал это обнаружение и добавил его как исключение из правил. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

     Подтверждение – если администратор обработал это обнаружение и подтвердил его. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

     Пусто – если администратор не обработал обнаружение.

- **Имя пользователя**

  Имя пользователя клиентского устройства, запустившего процесс, который сгенерировал обнаружение.

- **Обработан**

  Дата обнаружения аномалии.

- **Путь исходного процесса**

  Путь к исходному процессу, то есть к процессу, выполнившему действие (подобную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного процесса**

  Хеш SHA256 исходного файла процесса (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь исходного объекта**

  Путь к объекту, который запустил процесс (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного объекта**

  Хеш SHA256 исходного файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого процесса**

  Путь к целевому процессу (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого процесса**

  Хеш SHA256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого объекта**

  Путь к целевому объекту (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого объекта**

  Хеш SHA256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

Чтобы просмотреть свойства каждого элемента:

1. В главном окне приложения перейдите в раздел **Операции** → **Хранилища**.
2. Перейдите по ссылке **Правила срабатываний в статусе Интеллектуальное обучение**.
3. В открывшемся окне выберите нужный объект.
4. Перейдите по ссылке **Свойства**.

В открывшемся окне свойств объекта отображается информация выбранного элемента.

Вы можете подтвердить или добавить в исключения любой объект в списке, обнаруженный правилами Адаптивного контроля аномалий.

Чтобы подтвердить объект,

выберите один или несколько элементов в списке обнаружений и нажмите на кнопку **Подтвердить**.

Статус элементов будет изменен на **Подтверждается**.

Ваше подтверждение влияет на статистику, используемую правилами (подробную информацию см. в документации Kaspersky Endpoint Security для Windows).

Чтобы добавить объект в исключения,

выберите один или несколько элементов в списке обнаружений и нажмите на кнопку **Исключить**.

В результате запустится мастер добавления исключений. Следуйте далее указаниям мастера.

Если вы отклоните или подтвердите объект, он будет исключен из списка обнаружений после следующей синхронизации клиентского устройства с Сервером администрирования и больше не будет отображаться в списке.

Добавление исключений в правила Адаптивного контроля аномалий

Мастер добавления исключений позволяет добавлять исключения из правил Адаптивного контроля аномалий для Kaspersky Endpoint Security для Windows.

Чтобы запустить мастер добавления исключений в папке Адаптивный контроль аномалий:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Правила срабатываний в статусе Интеллектуальное обучение**.
2. В открывшемся окне в контекстном меню одного или нескольких элементов в списке обнаружений нажмите на кнопку **Исключить**.

   За один раз можно добавить до 1000 исключений. Если вы выберете больше элементов и попытаетесь добавить их в исключения, появится сообщение об ошибке.

   В результате запустится мастер добавления исключений. Для продолжения работы мастера нажмите на кнопку **Далее**.

Управление группами администрирования

Этот раздел содержит информацию о работе с группами администрирования.

Вы можете выполнять с группами администрирования следующие действия:

- добавлять в состав группы администрирования произвольное количество вложенных групп любых уровней иерархии;
- добавлять в состав групп администрирования устройства;

- изменять иерархию групп администрирования путем перемещения отдельных устройств и целых групп в другие группы;
- удалять из состава групп администрирования вложенные группы и устройства;
- добавлять в состав групп администрирования подчиненные и виртуальные Серверы администрирования;
- переносить устройства из состава групп администрирования одного Сервера в группы администрирования другого Сервера;
- определять, какие приложения "Лаборатории Касперского" будут автоматически устанавливаться на устройства, включаемые в состав группы.

Эти действия можно выполнять, только если у вас есть право **Изменение** в области **Управление группами администрирования для групп**, которыми вы хотите управлять, или для Сервера администрирования, к которому относятся эти группы.

Создание групп администрирования

Исходно иерархия групп администрирования содержит только одну группу администрирования, которая называется **Управляемые устройства**. Вы можете добавлять устройства и подгруппы в состав группы **Управляемые устройства**.

Чтобы создать группу администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами → Иерархия групп**.
2. В иерархии выберите группу администрирования, которая должна включать новую группу администрирования.
3. Нажмите на кнопку **Добавить**.
4. В открывшемся окне введите имя группы и нажмите на кнопку **ОК**.

Новая группа администрирования, с указанным именем, появится в иерархии групп администрирования.

Приложение позволяет создавать структуру групп администрирования на основе структуры Active Directory или структуры доменной сети. Также вы можете создавать структуру групп из текстового файла.

Чтобы создать структуру групп администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами → Иерархия групп**.
2. Нажмите на кнопку **Импортировать**.

В результате запускается мастер создания структуры групп администрирования. Следуйте далее указаниям мастера.

Автоматическая установка приложений на устройства группы администрирования

Вы можете указать, какие инсталляционные пакеты нужно использовать для автоматической удаленной установки приложений "Лаборатории Касперского" на клиентские устройства в группе администрирования.

Чтобы настроить автоматическую установку приложений на устройства в группе администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп** и нажмите на имя нужной группы администрирования.
2. В открывшемся окне свойств перейдите на вкладку **Автоматическая установка**.
3. Выберите инсталляционные пакеты приложений, которые необходимо установить на устройства, и нажмите на кнопку **Сохранить**.

   Если выбрано несколько инсталляционных пакетов одного и того же приложения, отличающихся только версиями, сохраняется инсталляционный пакет с последней версией.

После выбора инсталляционных пакетов, для каждого приложения создается группа задач для установки приложений на устройства в группе администрирования. Эти задачи будут запускаться на клиентских устройствах сразу после их добавления в группу администрирования.

Перемещение групп администрирования

Вы можете перемещать вложенные группы администрирования внутри иерархии групп.

Группа администрирования перемещается вместе со всеми вложенными группами, подчиненными Серверами администрирования, устройствами, групповыми политиками и задачами. Приложение применяет все параметры, соответствующие ее новому положению в иерархии групп администрирования.

Имя группы должно быть уникальным в пределах одного уровня иерархии. Если в папке, в которую вы перемещаете группу администрирования, уже существует группа с аналогичным названием, перед перемещением название группы нужно изменить. Если вы предварительно не изменили название перемещаемой группы, к ее названию при перемещении автоматически добавляется окончание вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Вы не можете изменить название группы **Управляемые устройства** или переместить ее.

Чтобы переместить группу администрирования на другой уровень иерархии групп администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп** и установите флажок рядом с группой администрирования, которую вы хотите переместить.
2. В панели инструментов нажмите на кнопку **Переместить**.
3. В открывшемся окне выберите, куда вы хотите переместить группу администрирования, и нажмите на кнопку **Переместить**.

Окно закрывается и группа администрирования перемещается на другой уровень в иерархии групп.

Удаление групп администрирования

Если вы удалите группу администрирования, содержащую подчиненные Серверы администрирования, вложенные группы, клиентские устройства, групповые задачи или политики, созданные для этой группы, все они также будут удалены.

Перед удалением группы администрирования требуется удалить из ее состава подчиненные Серверы администрирования, вложенные группы и клиентские устройства.

Чтобы удалить группу администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп** и установите флажок рядом с группой администрирования, которую вы хотите удалить.
2. В панели инструментов нажмите на кнопку **Удалить**.

Группа администрирования удалена.

Политики и профили политик

Политика – это набор параметров приложения "Лаборатории Касперского", которые применяются к группе администрирования и ее подгруппе. Вы можете установить несколько приложений "Лаборатории Касперского" на устройства группы администрирования. Kaspersky Security Center предоставляет по одной политике для каждого приложения "Лаборатории Касперского" в группе администрирования. Политика имеет один из следующих статусов:

Статус политики

Состояние	Описание
Активная	Это текущая политика, которая применяется к устройству. Для приложения "Лаборатории Касперского" в каждой группе администрирования может быть активна только одна политика. Значения параметров активной политики приложения "Лаборатории Касперского" применяются к устройству.
Неактивная	Политика, которая в настоящее время не применяется к устройству.
Для автономных пользователей	Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.

Политики действуют по следующим правилам:

- Для одного приложения можно настроить несколько политик с различными значениями.
- Для одного приложения может быть активна только одна политика.
- Политика может иметь дочерние политики.

Вы можете использовать политики для подготовки к экстренным ситуациям, например, к вирусной атаке. Например, если происходит атака через флеш-накопители USB, можно активировать политику, блокирующую доступ к флеш-накопителям. В этом случае текущая активная политика автоматически становится неактивной.

Чтобы не поддерживать большое число политик, например, когда в разных случаях предполагается изменение только нескольких параметров, вы можете использовать профили политик.

Профиль политики – это именованное подмножество параметров политики, которые заменяют значения параметров политики. Профиль политики влияет на формирование эффективных параметров управляемого устройства. *Эффективные параметры* – это набор параметров политики, параметров профиля политики и параметров локального приложения, которые в настоящее время применяются к устройству.

Профили политик работают по следующим правилам:

- Профиль политики вступает в силу при возникновении определенного условия активации.
- Профили политики содержат значения параметров, которые отличаются от параметров политики.
- Активация профиля политики изменяет эффективные параметры управляемого устройства.
- В политике может быть не более 100 профилей политик.

Вы не можете создать политику Сервера администрирования.

Блокировка (замок) и заблокированные параметры

У каждого параметра политики есть значок замка (). В таблице ниже показаны состояния значка замка:

Статусы значка замка

Состояние	Описание
Undefined	Если рядом с параметром отображается значок открытого замка и переключатель выключен, параметр не указан в политике. Пользователь может изменить эти параметры в интерфейсе управляемого приложения. Такие параметры называются *разблокированными*.
Enforce	Если рядом с параметром отображается закрытый значок замка и переключатель включен, параметр применяется к устройствам, на которых применяется политика. Пользователь не может изменять значения этих параметров в интерфейсе управляемого приложения. Такие параметры называются *заблокированными*.

Рекомендуется заблокировать параметры политики, которые вы хотите применить к управляемым устройствам. Разблокированные параметры политики могут быть переназначены параметрами приложения "Лаборатории Касперского" на управляемом устройстве.

Вы можете использовать значок замка для выполнения следующих действий:

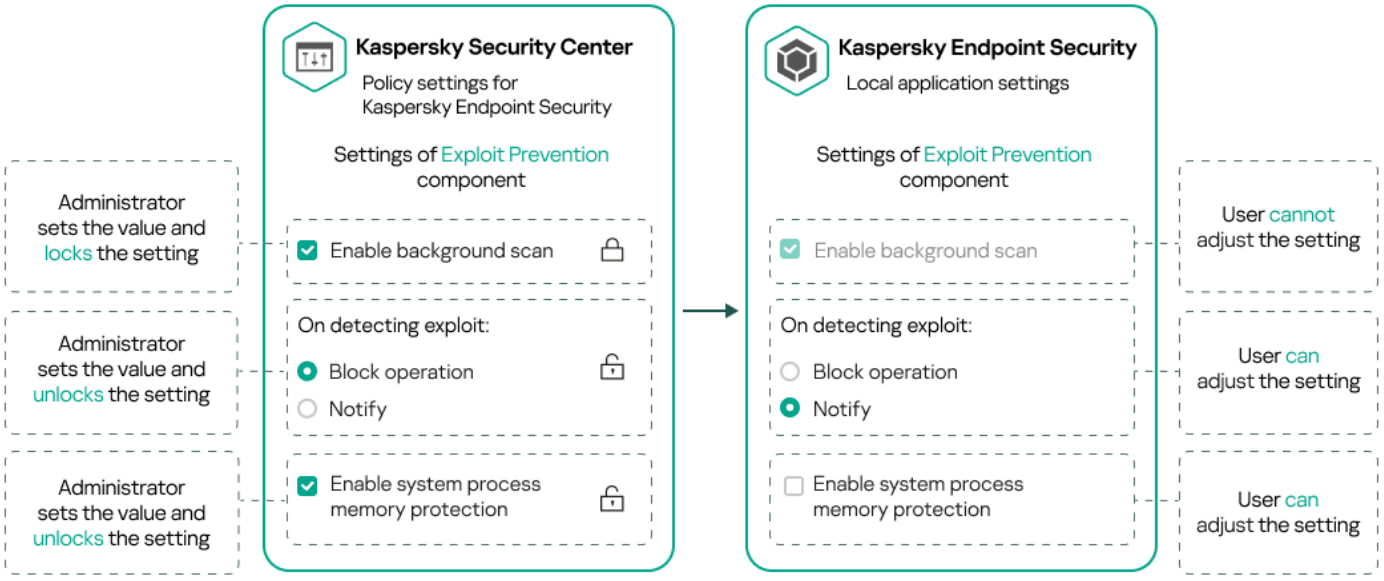
- Блокировка параметров для политики подгруппы администрирования.
- Блокировка параметров приложения "Лаборатории Касперского" на управляемом устройстве.

Таким образом, заблокированный параметр используется в эффективных параметрах на управляемом устройстве.

Применение эффективных параметров включает в себя следующие действия:

- Управляемое устройство применяет значения параметров приложения "Лаборатории Касперского".
- Управляемое устройство применяет заблокированные значения параметров политики.

Политика и управляемое приложение "Лаборатории Касперского" содержат одинаковый набор параметров. При настройке параметров политики параметры приложения "Лаборатории Касперского" меняют значения на управляемом устройстве. Вы не можете изменить заблокированные параметры на управляемом устройстве (см. рисунок ниже):



Замки и параметры приложения "Лаборатории Касперского"

Наследование политик и профилей политик

В этом разделе представлена информация об иерархии и наследовании политик и профилей политик.

Иерархия политик

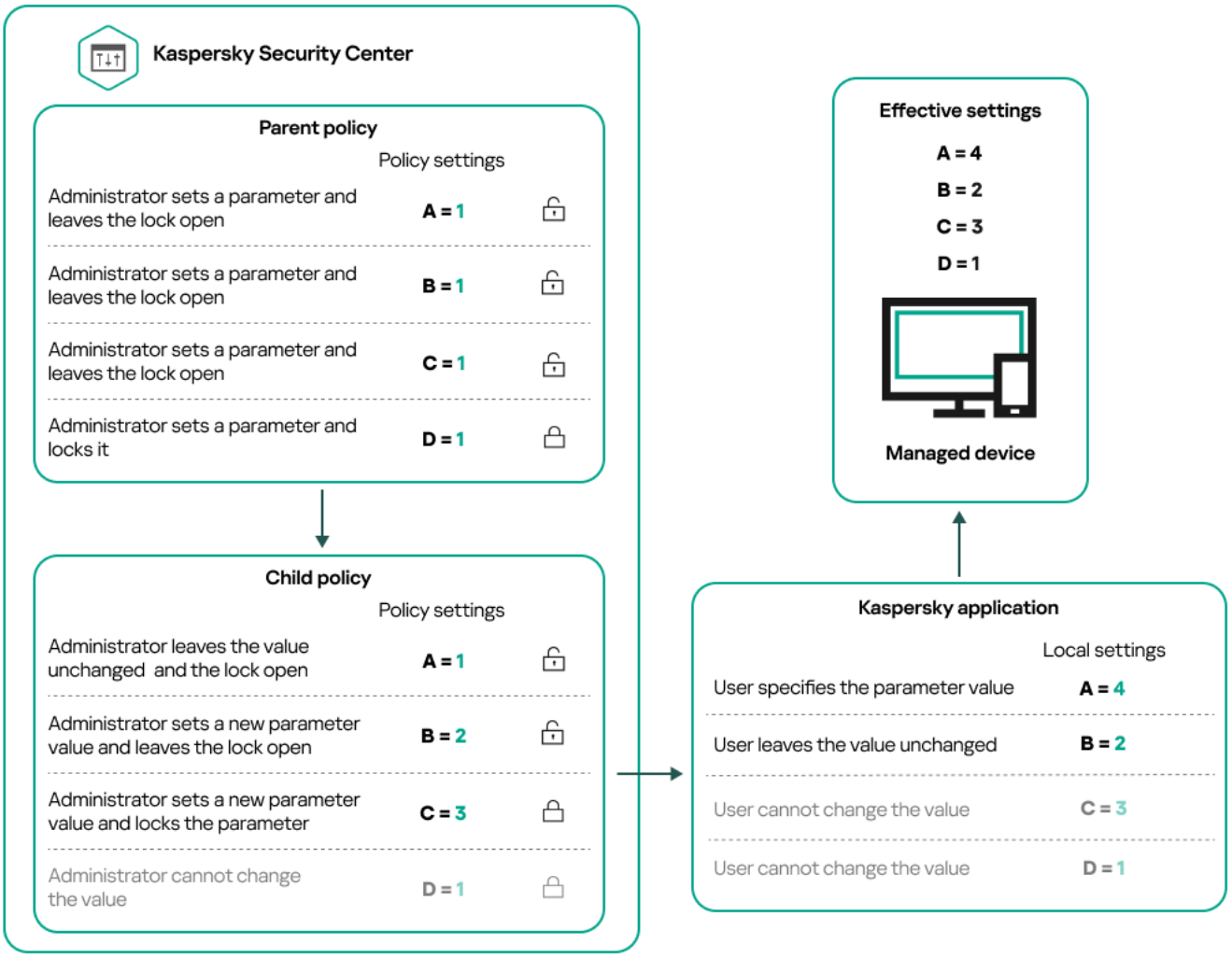
Если для разных устройств требуются разные параметры, вы можете объединить устройства в группы администрирования.

Вы можете указать политику для отдельной группы администрирования. Параметры политики можно *унаследовать*. Наследование – это получение значений параметров политики в подгруппах (дочерних группах) от вышестоящей политики (родительской) группы администрирования.

Политика, созданная для родительской группы, также называется *родительской политикой*. Политика, созданная для подгруппы (дочерней группы), также называется *дочерней политикой*.

По умолчанию на Сервере администрирования существует как минимум одна группа администрирования управляемых устройств. Если вы хотите создать группы администрирования, они создаются как подгруппы (дочерние группы) в группе Управляемые устройства.

Политики одного и того же приложения действуют друг на друга по иерархии групп администрирования. Заблокированные параметры из политики вышестоящей (родительской) группы администрирования будут переназначать значения параметров политики подгруппы (см. рисунок ниже).

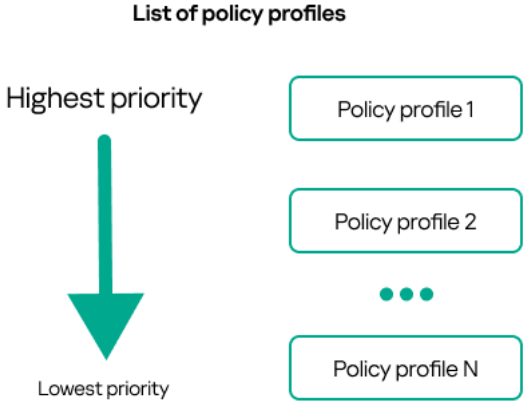


Иерархия политик

Профили политик в иерархии политик

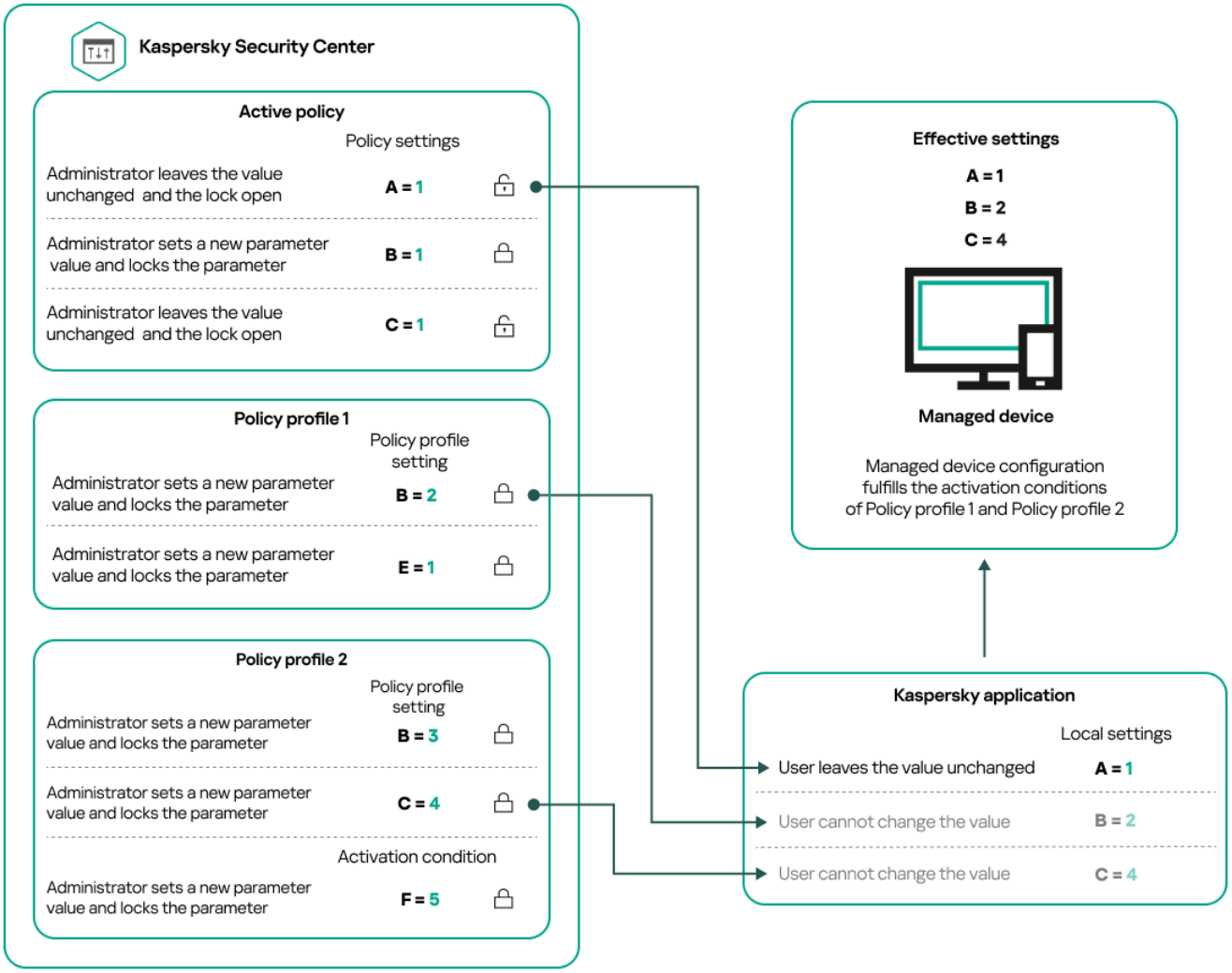
Профили политики имеют следующие условия назначения приоритета:

- Положение профиля в списке профилей политики обозначает его приоритет. Вы можете изменить приоритет профиля политики. Самая высокая позиция в списке обозначает самый высокий приоритет (см. рисунок ниже).



Определение приоритета профиля политики

- Условия активации профилей политик не зависят друг от друга. Одновременно можно активировать несколько профилей политик. Если несколько профилей политики влияют на один и тот же параметр, устройство использует значение параметра из профиля политики с наивысшим приоритетом (см. рисунок ниже).



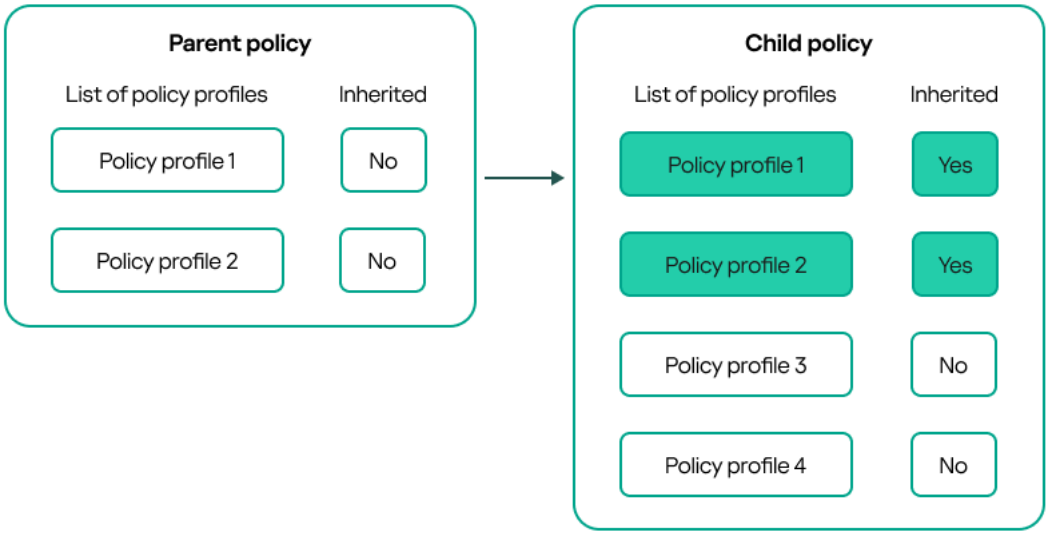
Конфигурация управляемого устройства соответствует условиям активации нескольких профилей политик

Профили политик в иерархии наследования

Профили политик из политик разных уровней иерархии соответствуют следующим условиям:

- Политика нижнего уровня наследует профили политики из политики более высокого уровня. Профиль политики, унаследованный от политики более высокого уровня, получает более высокий приоритет, чем уровень исходного профиля политики.

- Вы не можете изменить приоритет унаследованного профиля политики (см. рисунок ниже).



Наследование параметров профилей политики

Профили политики с одинаковыми именами

Если на разных уровнях иерархии есть две политики с одинаковыми именами, эти политики работают в соответствии со следующими правилами:

- Заблокированные параметры и условие активации профиля для профиля политики более высокого уровня изменяют параметры и условие активации профиля для профиля политики более низкого уровня (см. рисунок ниже).

Дочерний профиль наследует значения параметров из родительского профиля политики

- Разблокированные параметры и условие активации профиля для профиля политики более высокого уровня не изменяют параметры и условие активации профиля для профиля политики более низкого уровня.

Как параметры реализованы на управляемом устройстве

Применения эффективных параметров на управляемом устройстве можно описать следующим образом:

- Значения всех незаблокированных параметров берутся из политики.
- Затем они перезаписываются значениями параметров управляемого приложения.
- Далее применяются заблокированные значения параметров из действующей политики. Значения заблокированных параметров изменяют значения разблокированных действующих параметров.

Управление политиками

В этом разделе описывается управление политиками и предоставляется информация о просмотре списка политик, создании политики, изменении политики, копировании политики, перемещении политики, принудительной синхронизации, просмотре диаграммы состояния распространения политики и удалении политики.

Просмотр списка политик

Вы можете просмотреть список политик, созданных на Сервере администрирования или в любой группе администрирования.

Чтобы просмотреть список политик:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.
2. В списке групп администрирования выберите группу администрирования, для которой вы хотите просмотреть список политик.

Политики отобразятся в виде таблицы. Если политик нет, отобразится пустая таблица. Вы можете отображать или скрывать столбцы таблицы, изменять их порядок, просматривать только строки, которые содержат указанное вами значение, или использовать поиск.

Создание политики

Вы можете создавать политики, а также изменять или удалять существующие политики.

> Вы не можете создать политику Сервера администрирования.

Чтобы создать политику:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Выберите группу администрирования, для которой нужно создать политику:
   - Для корневой группы.

     В этом случае вы можете перейти к следующему шагу.
   - Для подгруппы:

     a. Нажмите на кнопку **Показать иерархию** в верхней части страницы.

     Название кнопки изменится на **Скрыть иерархию**.

     b. В открывшемся окне нажмите на название нужной подгруппы.

   Путь к выбранной группе отображается в верхней части страницы. Чтобы перейти к группе администрирования, нажмите на ссылку с названием группы. По умолчанию последняя ссылка в пути неактивна. Также вы можете закрыть окно иерархии, нажав на кнопку **Скрыть иерархию**.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Выберите приложение**.
4. Выберите приложение, для которого требуется создать политику.
5. Нажмите на кнопку **Далее**.

   Откроется окно параметров новой политики на вкладке **Общие**.

6. При желании вы можете изменить следующие параметры политики, заданные по умолчанию: имя, состояние и наследование.

7. Выберите вкладку **Параметры приложения**.

   Или нажмите на кнопку **Сохранить**, чтобы выйти. Политика появится в списке политик, и вы сможете изменить ее свойства позже.

8. В левой области вкладки **Параметры приложения** выберите нужный вам раздел и в панели результатов измените параметры политики. Вы можете изменить параметры политики в каждом разделе.

   Параметры зависят от приложения, для которого вы создаете политику. Подробную информацию см. в следующих источниках:

   - Настройка Сервера администрирования
   - Параметры политики Агента администрирования
   - Документация Kaspersky Endpoint Security для Windows

   Подробнее о параметрах других приложений безопасности см. в документации к соответствующему приложению.

   Чтобы отменить изменения, вы можете нажать на кнопку **Отмена**.

9. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения политики.

В результате добавленная политика отображается в списке политик. После создания политики события изменения политик экспортируются в SIEM-систему, если этот параметр включен.

Изменение политики

Чтобы изменить политику:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

2. Выберите политику, которую требуется изменить.

   Откроется окно свойств политики.

3. Укажите общие параметры и параметры приложения, для которого вы создаете политику. Подробную информацию см. в следующих источниках:

   - Настройка Сервера администрирования
   - Параметры политики Агента администрирования
   - Документация Kaspersky Endpoint Security для Windows

   Подробнее о параметрах других приложений безопасности см. в документации к этим приложениям.

4. Нажмите на кнопку **Сохранить**.

   Отобразится уведомление: **Политика сохраняется и распространяется по иерархии Серверов администрирования**.

   Если политика прошла проверку, отображается уведомление: **Политика сохранена**.

Если политика не проходит проверку, отображается следующее уведомление: **Не удалось сохранить и распространить политику через иерархию Серверов администрирования. Обратитесь в Службу технической поддержки**. Вы можете просмотреть и изменить параметры политики, а затем повторить попытку. Если проблема продолжает сохраняться, обратитесь в Службу технической поддержки.

Изменения политики будут сохранены в свойствах политики и будут отображаться в разделе **История ревизий**. После изменения политики события изменения политик экспортируются в SIEM-систему, если этот параметр включен.

При необходимости вы можете сравнить ревизии политики. Параметр доступен для политик Сервера администрирования, Агента администрирования, Kaspersky Endpoint Security для Windows (начиная с версии веб-плагина 14.0) и Kaspersky Endpoint Security для Mac (начиная с версии веб-плагина 12.2.1 Patch A).

Общие параметры политик

Общие

На вкладке **Общие** можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
  - **Активна**
  - **Для автономных пользователей**

    Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.
  - **Неактивна**

    Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.
- В блоке **Наследование параметров** можно настроить параметры наследования политики:
  - **Наследовать параметры родительской политики**

    Если параметр включен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

    По умолчанию параметр включен.
  - **Обеспечить принудительное наследование параметров для дочерних политик**

    Если параметр включен, после применения изменений в политике будут выполнены следующие действия:
    - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
    - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически включен параметр **Наследовать параметры родительской политики**.

    Когда параметр включен, значения параметров дочерних политик недоступны для изменения.

    По умолчанию параметр выключен.

Настройка событий

На вкладке **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на вкладках:

- **Критическое**

  Раздел **Критическое** не отображается в свойствах политики Агента администрирования.

- **Отказ функционирования**

- **Предупреждение**

- **Информационное сообщение**

В каждом разделе в списке событий отображаются названия событий и время хранения событий на Сервере администрирования по умолчанию (в днях). Нажав на тип события, вы можете указать следующие параметры:

- **Регистрация событий**

  Вы можете указать количество дней хранения событий и выбрать, где хранить события:

  - **Хранить в базе данных Сервера администрирования в течение (сут)**

  - **Хранить в журнале событий ОС на устройстве**

- **Уведомления о событиях**

  Вы можете выбрать, хотите ли вы получать уведомления о событии по электронной почте.

  По умолчанию используются параметры уведомлений, указанные на вкладке свойств Сервера администрирования (например, адрес получателя). Вы можете изменить эти параметры на вкладке **Электронная почта**.

На вкладке **Настройка событий** отображаются уведомления при добавлении новых типов событий (например, в новой версии приложения), а также можно применить новые параметры, нажав на кнопку **Сохранить** или **Сохранить и закрыть**.

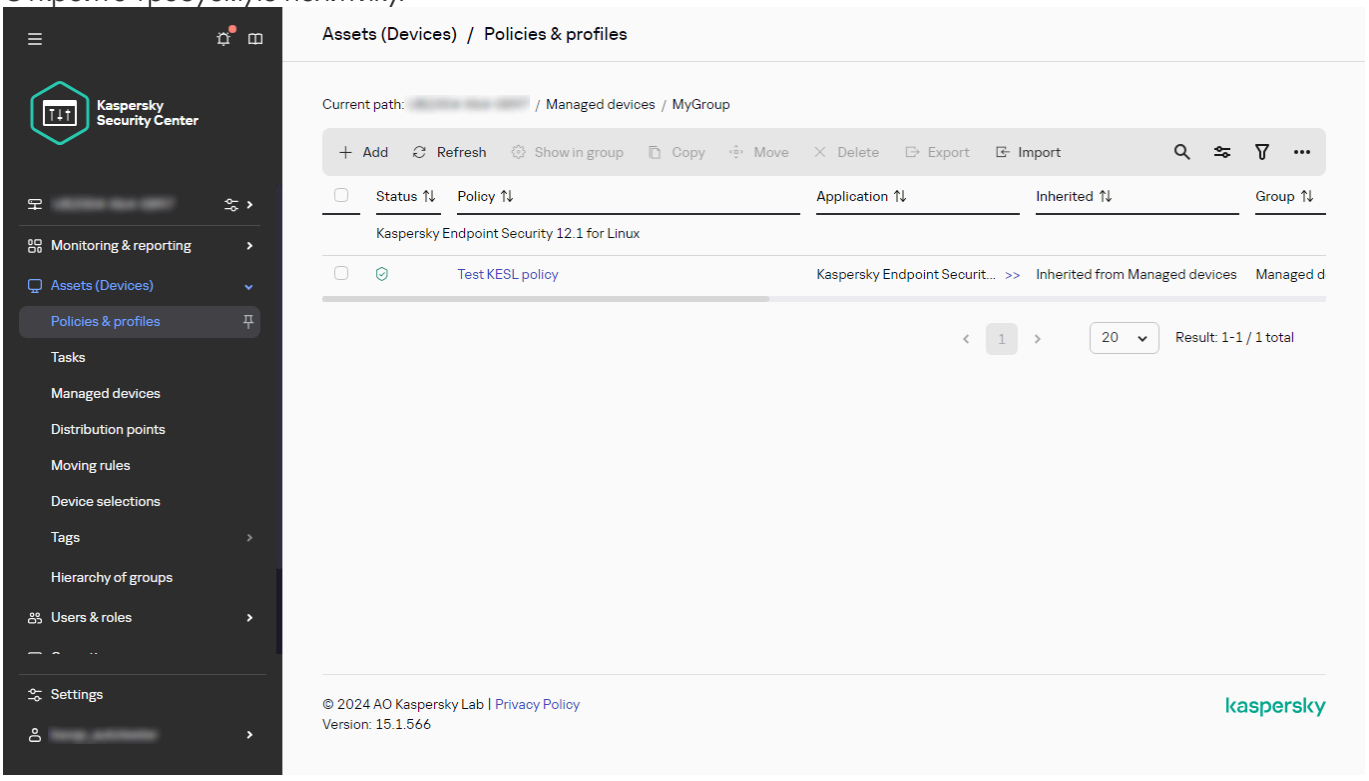
История ревизий

На вкладке **История ревизий** вы можете просмотреть список ревизий политики, сравнить ревизии политики и при необходимости откатить изменения политики.

Включение и выключение параметра наследования политики

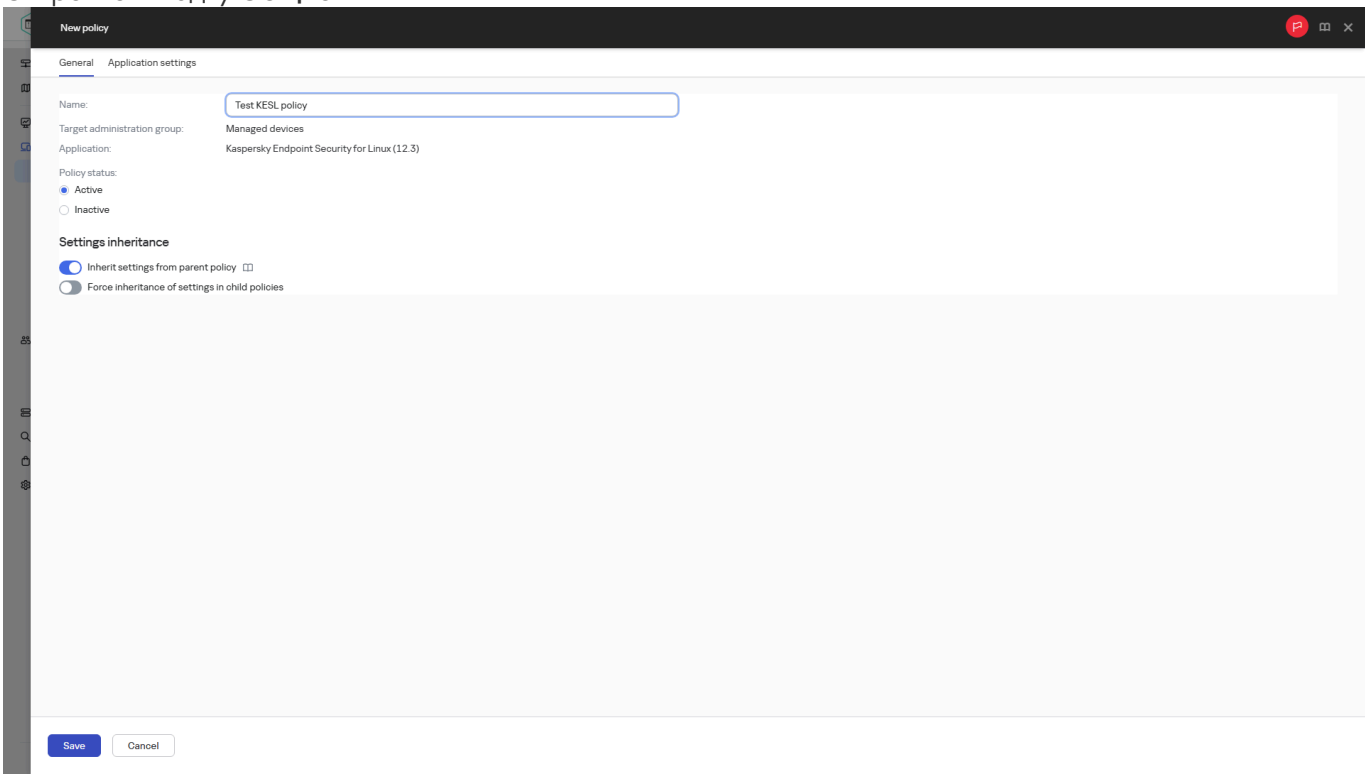
Чтобы включить или выключить параметр наследования в политике:

1. Откройте требуемую политику.



Список политик

2. Откройте вкладку **Общие**.



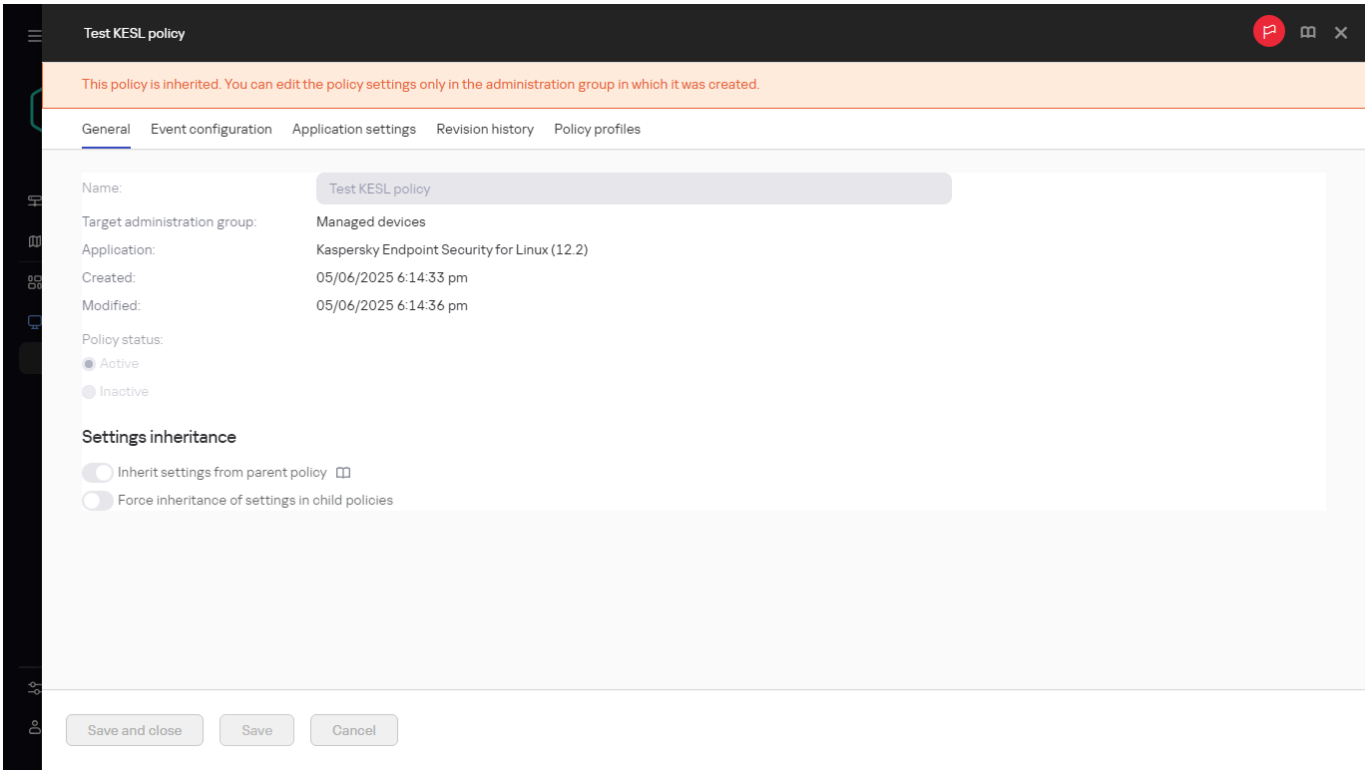
Создание политики

3. Включение или выключение наследования политики:

   - Если вы включили параметр **Наследовать параметры родительской политики** для дочерней группы и администратор заблокировал некоторые параметры в родительской политике, то вы не можете изменить эти параметры политики для дочерней политики.

   - Если вы выключили параметр **Наследовать параметры родительской политики** для дочерней политики, то вы можете изменить все параметры в дочерней политике, даже если некоторые параметры "заблокированы" в родительской политике.

   - Если в родительской группе включен параметр **Обеспечить принудительное наследование параметров для дочерних политик**, это включит параметр **Наследовать параметры родительской политики** для каждой дочерней политики. В этом случае вы не можете выключить этот параметр для дочерних политик. Все параметры, которые заблокированы в родительской политике, принудительно наследуются в дочерних группах, и вы не можете изменить эти параметры в дочерних группах.



Заблокированные параметры политик

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, или нажмите на кнопку **Отмена**, чтобы отклонить изменения.

По умолчанию, параметр **Наследовать параметры родительской политики** включен для новой политики.

Если у политики имеются профили, все дочерние политики наследуют эти профили.

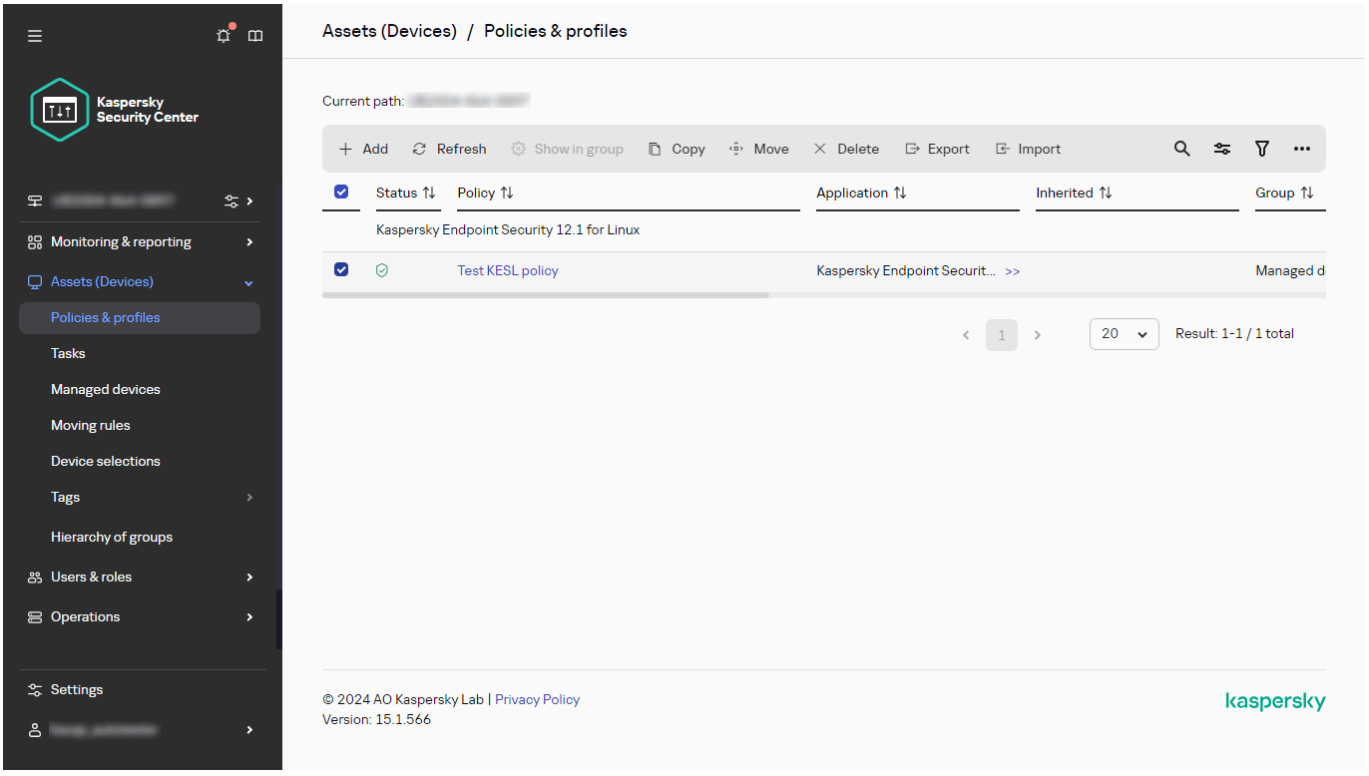
Копирование политики

Вы можете копировать политики из одной группы администрирования в другую.

Чтобы скопировать политику в другую группу администрирования:

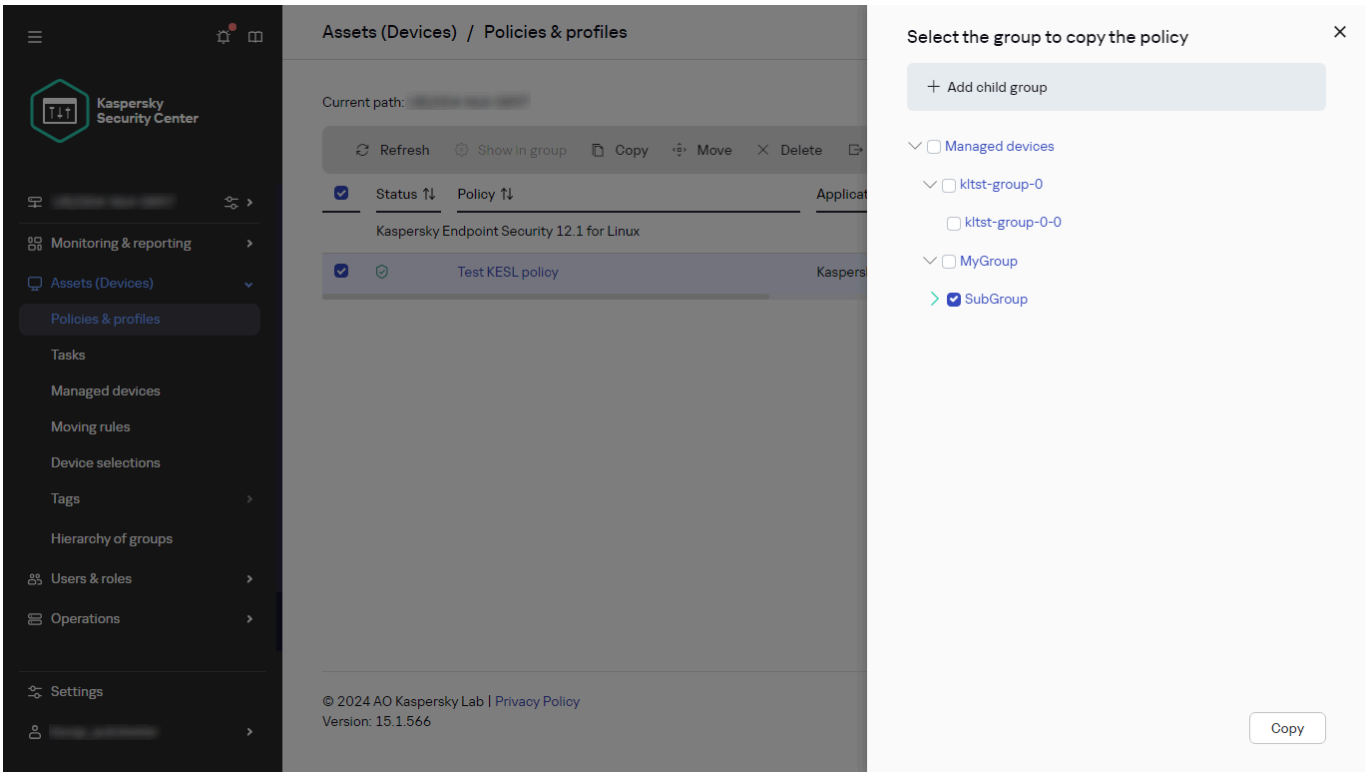
1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

2. Установите флажок напротив политики (или политик), которую требуется скопировать.



3. Нажмите на кнопку **Копировать**.

   В правой части экрана отображается дерево групп администрирования.



4. В дереве выберите целевую группу, то есть группу, в которую вы хотите скопировать политику (или политики).

5. Нажмите на кнопку **Копировать** внизу экрана.

6. Нажмите на кнопку **OK**, чтобы подтвердить операцию.

Политика (политики) и все ее профили скопированы в целевую группу администрирования. Каждая скопированная политика в целевой группе принимает статус **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

Перемещение политики

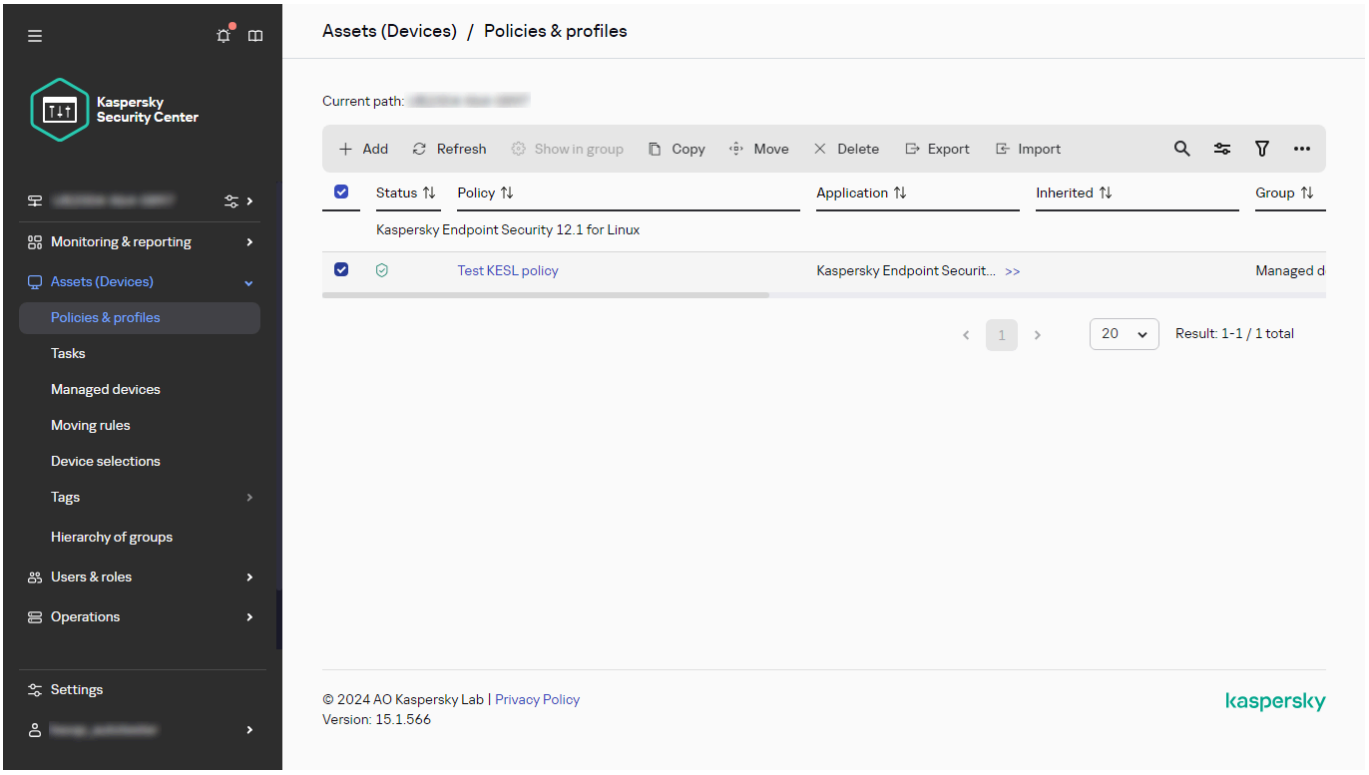
Вы можете перемещать политики из одной группы администрирования в другую. Например, вы хотите удалить одну группу администрирования, но использовать ее политики для другой группы администрирования. В этом случае вам может потребоваться, перед удалением старой группы администрирования, переместить политику из старой группы администрирования в новую.

> При перемещении политики в другую группу администрирования история изменений политики удаляется. На вкладке **История ревизий** отображается информация только о последних изменениях.

Чтобы переместить политику в другую группу администрирования:

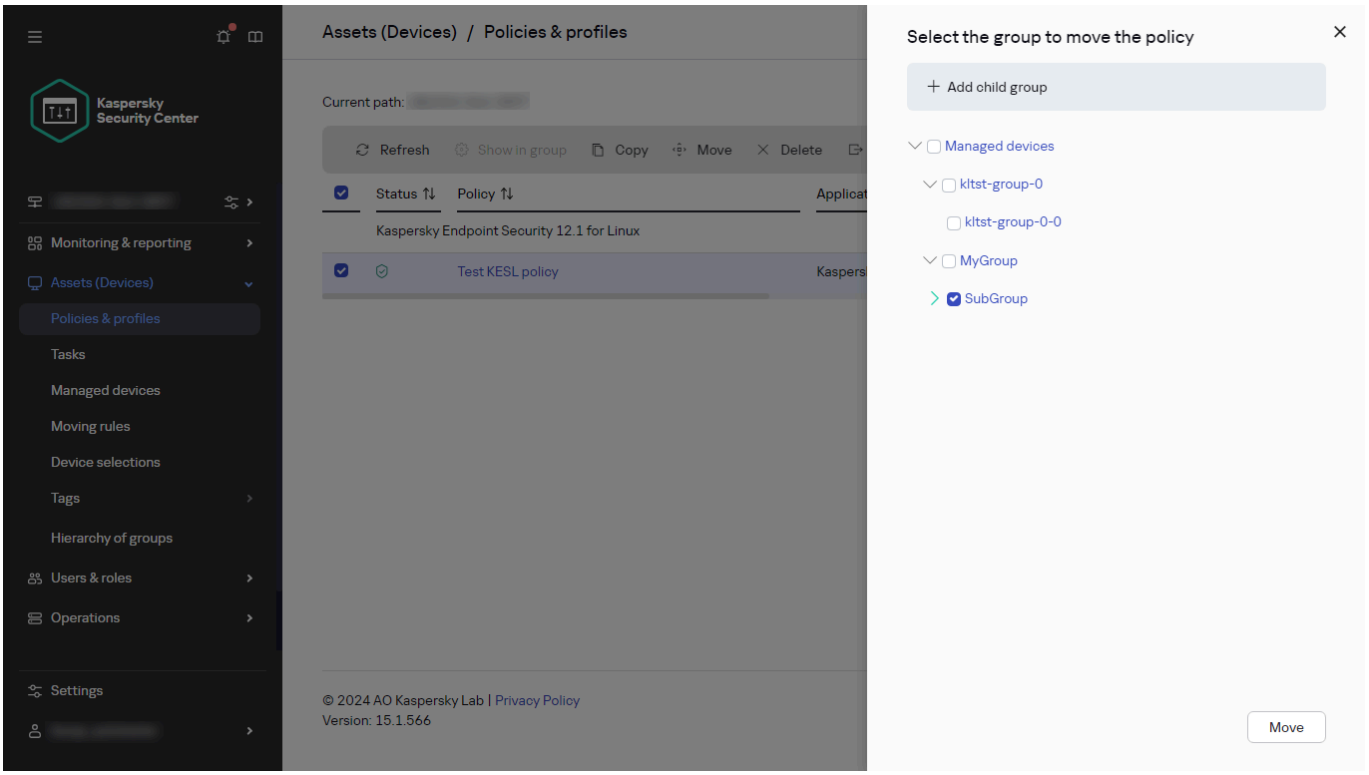
1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

2. Установите флажок напротив политики (или политик), которую требуется переместить.



3. Нажмите на кнопку **Переместить**.

   В правой части экрана отображается дерево групп администрирования.



4. В дереве выберите целевую группу администрирования, то есть группу, в которую вы хотите переместить политику (или политики).

5. Нажмите на кнопку **Переместить** внизу экрана.

6. Нажмите на кнопку **OK**, чтобы подтвердить операцию.

   Если политика не унаследована из группы источника, она будет перемещена в целевую группу со всем профилями политики. Статус политики в целевой группе администрирования будет **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

   Если политика унаследована из группы источника, она останется в группе источника. Политика скопирована в целевую группу со всеми ее профилями. Статус политики в целевой группе администрирования будет **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

Экспорт политики

Open Single Management Platform позволяет сохранить политику, ее параметры и профили политики в файл KLP. Вы можете использовать файл KLP для импорта сохраненной политики как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

Чтобы экспортировать политику:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

2. Установите флажок рядом с политикой, которую вы хотите экспортировать.

   Невозможно экспортировать несколько политик одновременно. Если вы выберете более одной политики, кнопка **Экспортировать** будет неактивна.

3. Нажмите на кнопку **Экспортировать**.

4. В открывшемся окне **Сохранить как** укажите имя файла политики и путь. Нажмите на кнопку **Сохранить**.

   Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл политики автоматически сохраняется в папку **Загрузки**.

Импорт политики

Open Single Management Platform позволяет импортировать политику из файла KLP. Файл KLP содержит экспортированную политику, ее параметры и профили политики.

Чтобы импортировать политику:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

2. Нажмите на кнопку **Импортировать**.

3. Нажмите на кнопку **Обзор**, чтобы выбрать файл политики, который вы хотите импортировать.

4. В открывшемся окне укажите путь к файлу политики KLP и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл политики.

   Начнется обработка политики.

5. После успешной обработки политики выберите группу администрирования, к которой вы хотите применить политику.

6. Нажмите на кнопку **Завершить**, чтобы завершить импорт политики.

Появится уведомление с результатами импорта. Если политика успешно импортирована, вы можете перейти по ссылке **Подробнее** для просмотра свойств политики.

После успешного импорта политика отображается в списке политик. Также импортируются параметры и профили политики. Независимо от статуса политики, выбранной при экспорте, импортируемая политика неактивна. Вы можете изменить статус политики в свойствах политики.

Если параметры политики приложения содержат пароли, такую политику невозможно применить после импорта на другой Сервер Администрирования. В этом случае измените пароли в импортированной политике для ее применения.

Если имя новой импортированной политики идентично имени существующей политики, имя импортированной политики расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Просмотр диаграммы состояния применения политики

В Kaspersky Security Center Cloud Console вы можете просматривать состояние применения политики на каждом устройстве на диаграмме.

Чтобы просмотреть статус применения политики на каждом устройстве:

1. В главном окне приложения перейдите в раздел **Управление активами → Политики**.
2. Установите флажок рядом с именем политики, для которой вы хотите просмотреть состояние применения на устройстве.
3. В появившемся меню перейдите по ссылке **Результаты применения**.

   Откроется окно **Результат распространения <название политики>**.
4. В открывшемся окне **Результат распространения <название политики>** отображается **Описание статуса (если доступно)**.

Вы можете изменить количество результатов, отображаемых в списке результатов применения политики. Максимальное количество устройств равно 100 000.

Чтобы изменить количество устройств, отображаемых в списке с результатами применения политики:

1. В главном окне приложения перейдите в раздел **Параметры → Параметры интерфейса**.
2. В поле **Максимальное количество устройств, отображаемых в результатах распространения политики** введите количество устройств (до 100 000).

   По умолчанию количество устройств равно 5000.
3. Нажмите на кнопку **Сохранить**.

Параметры сохранены и применены.

Автоматическая активация политики по событию "Вирусная атака"

Чтобы политика активировалась автоматически при наступлении события "Вирусная атака":

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.
2. Выберите раздел **Вирусная атака**.
3. В панели справа перейдите по ссылке **Настроить активацию политик по возникновению события "Вирусная атака"**.

   Откроется окно **Активация политик**.
4. В разделе, к которому относится компонент обнаруживший вирусную атаку (антивирусы для рабочих станций и файловых серверов, антивирусы для почтовых серверов, антивирусы защиты периметра), выберите нужную вам запись и затем нажмите на кнопку **Добавить**.

   Откроется окно с группой администрирования **Управляемые устройства**.
5. Нажмите на значок шеврона (>) рядом с **Управляемые устройства**.

   Отобразится иерархия групп администрирования и их политик.
6. В иерархии групп администрирования и их политик нажмите на название политики (или политик), которая активируется при возникновении вирусной атаки.

   Чтобы выбрать все политики в списке или в группе, установите флажок рядом с требуемым именем.

7. Нажмите на кнопку **Сохранить**.

   Окно с иерархией групп администрирования и их политиками закрыто.

Выбранные политики добавляются в список политик, которые активируются при возникновении вирусной атаки. Выбранные политики активируются во время вирусной атаки независимо от того, активны они или неактивны.

В случае активации политики по событию Вирусная атака вернуться к предыдущей политике можно только вручную.

Принудительная синхронизация

Несмотря на то, что Kaspersky SIEM Cloud автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, в некоторых случаях требуется точно знать, выполнена ли синхронизация определенного устройства на данный момент.

Чтобы эта функция работала, необходимо включить параметр **Не разрывать соединение с Сервером администрирования** и/или использовать точку распространения в качестве push-сервера.

Синхронизация одного устройства

Чтобы осуществить принудительную синхронизацию между Сервером администрирования и управляемым устройством:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
2. Выберите имя устройства, которое требуется синхронизировать с Сервером администрирования.

   В открывшемся окне свойств выберите раздел **Общие**.
3. Нажмите на кнопку **Синхронизировать сейчас**.

Приложение выполняет синхронизацию выбранного устройства с Сервером администрирования.

Синхронизация нескольких устройств

Чтобы осуществить принудительную синхронизацию между Сервером администрирования и несколькими управляемыми устройствами:

1. Откройте список устройств группы администрирования или выборку устройств:

   - Запустите выборку устройств, чтобы просмотреть список устройств.

   - В главном окне приложения перейдите в разделе **Управление активами → Управляемые устройства** и выберите группу администрирования, содержащую устройства для синхронизации.

     - Для корневой группы вы можете перейти к следующему шагу.

     - Для подгруппы в верхней части страницы нажмите на кнопку **Показать иерархию** и в открывшемся окне нажмите на имя подгруппы.

       Путь к выбранной группе отображается в верхней части страницы. Чтобы перейти к группе администрирования, нажмите на ссылку с названием группы. По умолчанию последняя ссылка в пути неактивна. Также вы можете закрыть окно иерархии, нажав на кнопку **Скрыть иерархию**.

2. Установите флажки рядом с устройствами, которые требуется синхронизировать с Сервером администрирования.

3. Над списком управляемых устройств нажмите на кнопку с многоточием (...) и нажмите на кнопку **Синхронизировать сейчас**.

   Приложение выполняет синхронизацию выбранных устройств с Сервером администрирования.

4. В списке устройств проверьте, что время последнего подключения к Серверу администрирования для выбранных устройств изменилось на текущее время. Если время не изменилось, обновите содержимое страницы, нажав на кнопку **Обновить**.

Выбранные устройства синхронизированы с Сервером администрирования.

Просмотр времени доставки политики

После изменения политики для приложения "Лаборатории Касперского" на Сервере администрирования вы можете проверить, доставлена ли измененная политика на определенные управляемые устройства. Политика может быть доставлена во время регулярной или принудительной синхронизации.

Чтобы просмотреть дату и время доставки политики приложения на управляемые устройства:

1. В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства**.

2. Выберите имя устройства, которое требуется синхронизировать с Сервером администрирования.

   В открывшемся окне свойств выберите раздел **Общие**.

3. Перейдите на вкладку **Приложения**.

4. Выберите приложение, для которого требуется посмотреть дату синхронизации политики.

Откроется окно политики программы, с выбранным разделом **Общие**, и отобразится дата и время доставки политики.

Удаление политики

Вы можете удалить политику, если она больше не нужна. Вы можете удалить только неунаследованную политику в выбранной группе администрирования. Если политика унаследована, вы можете удалить ее только в группе администрирования, в которой она была создана.

Чтобы удалить политику:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Установите флажок рядом с именем политики, которую вы хотите удалить, и нажмите на кнопку **Удалить**.

   Кнопка **Удалить** становится неактивной (серой), если вы выбрали унаследованную политику.
3. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

Политика и все ее профили политики удалены. После удаления политики события изменения политик экспортируются в SIEM-систему, если этот параметр включен.

Управление профилями политик

В этом разделе описывается управление профилями политики и предоставляется информация о просмотре профилей политики, изменении приоритета профиля политики, создании профиля политики, копировании профиля политики, создании правила активации профиля политики, удалении, экспорте и импорте профиля политики.

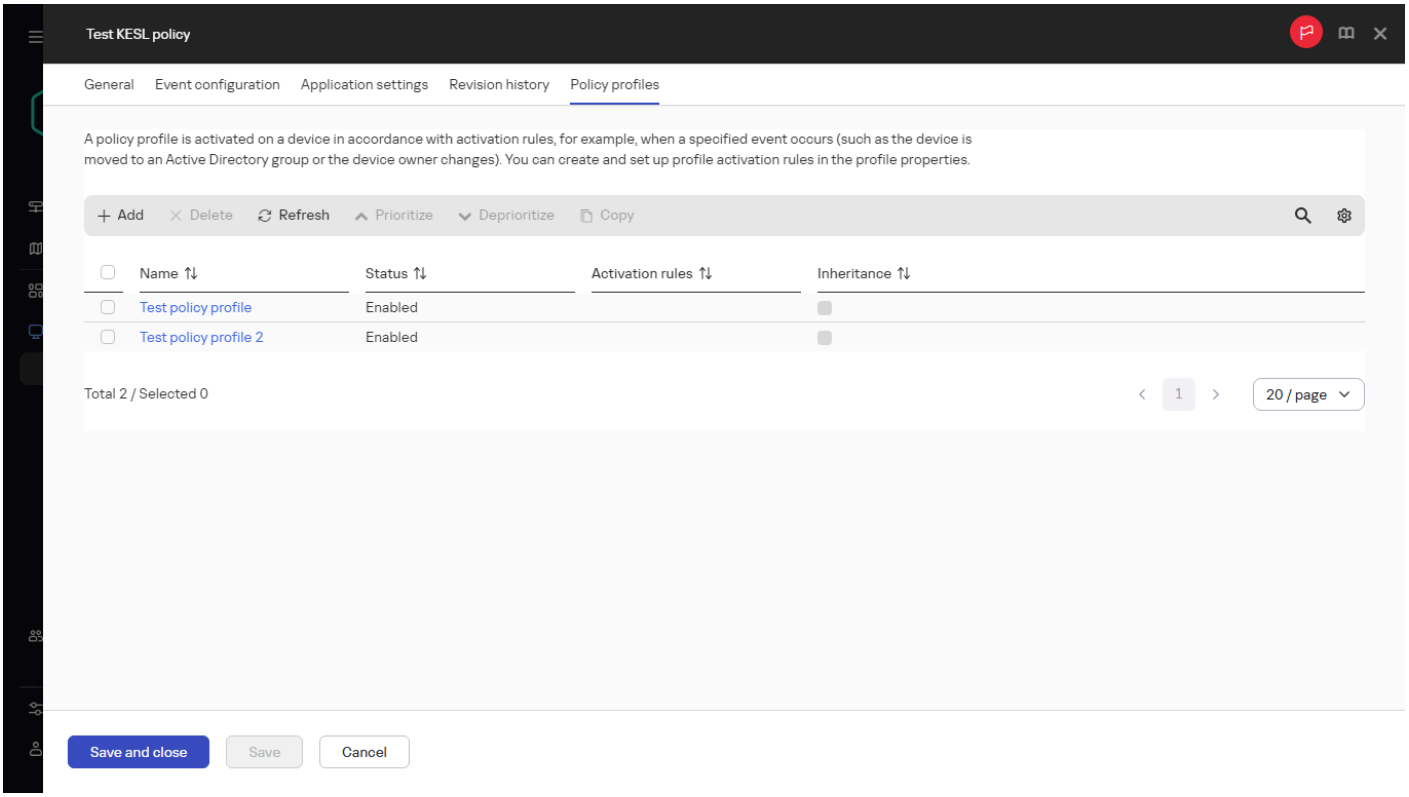
Просмотр профилей политики

Чтобы просмотреть профили политики:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Выберите политику, профили которой требуется просмотреть.

   Откроется окно свойств политики на вкладке **Общие**.
3. Откройте вкладку **Профили политики**.

Профили политики отобразятся в виде таблицы. Если у политики нет профилей политики, отобразится пустая таблица.



Список профилей политики

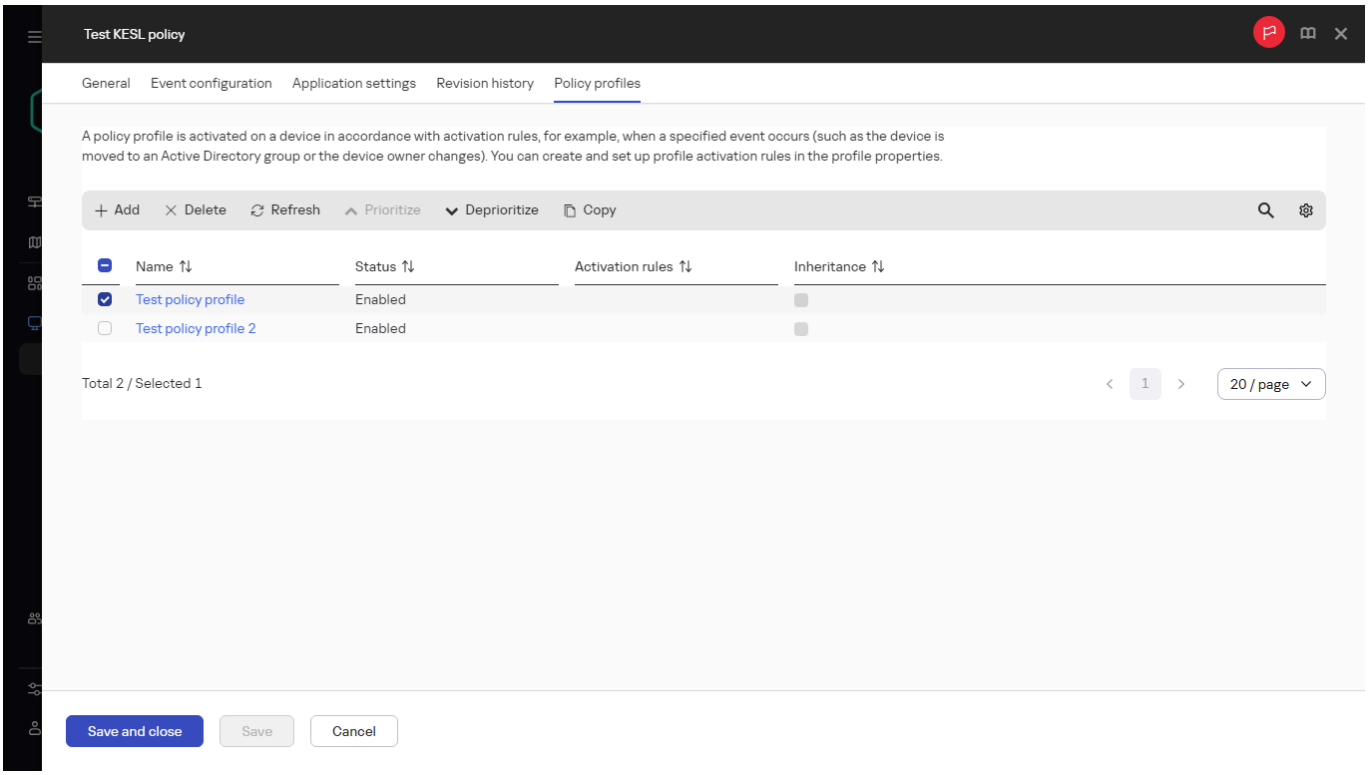
Изменение приоритета профиля политики

Чтобы изменить приоритет профиля политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.
2. На вкладке **Профили политики** установите флажок рядом с профилем политики, для которого требуется изменить приоритет.
3. Установите профиль политики на новую позицию в списке с помощью кнопок **Повысить приоритет** или **Понизить приоритет**.

   Чем выше расположен профиль политики в списке, тем выше его приоритет.



4. Нажмите на кнопку **Сохранить**.

Приоритет выбранного профиля политики изменен и применен.

Создание профиля политики

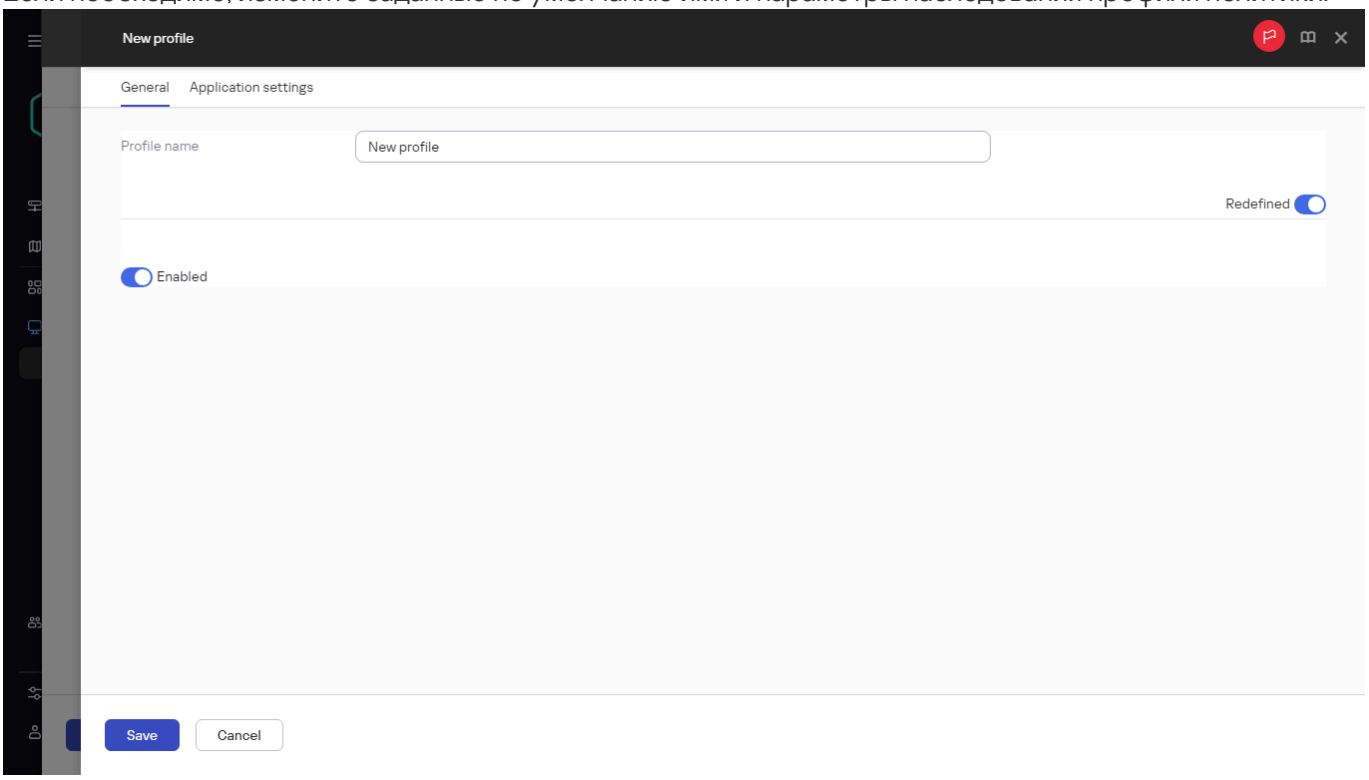
Чтобы создать профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики. Если у политики нет профилей политики, отобразится пустая таблица.

2. Нажмите на кнопку **Добавить**.

3. Если необходимо, измените заданные по умолчанию имя и параметры наследования профиля политики.



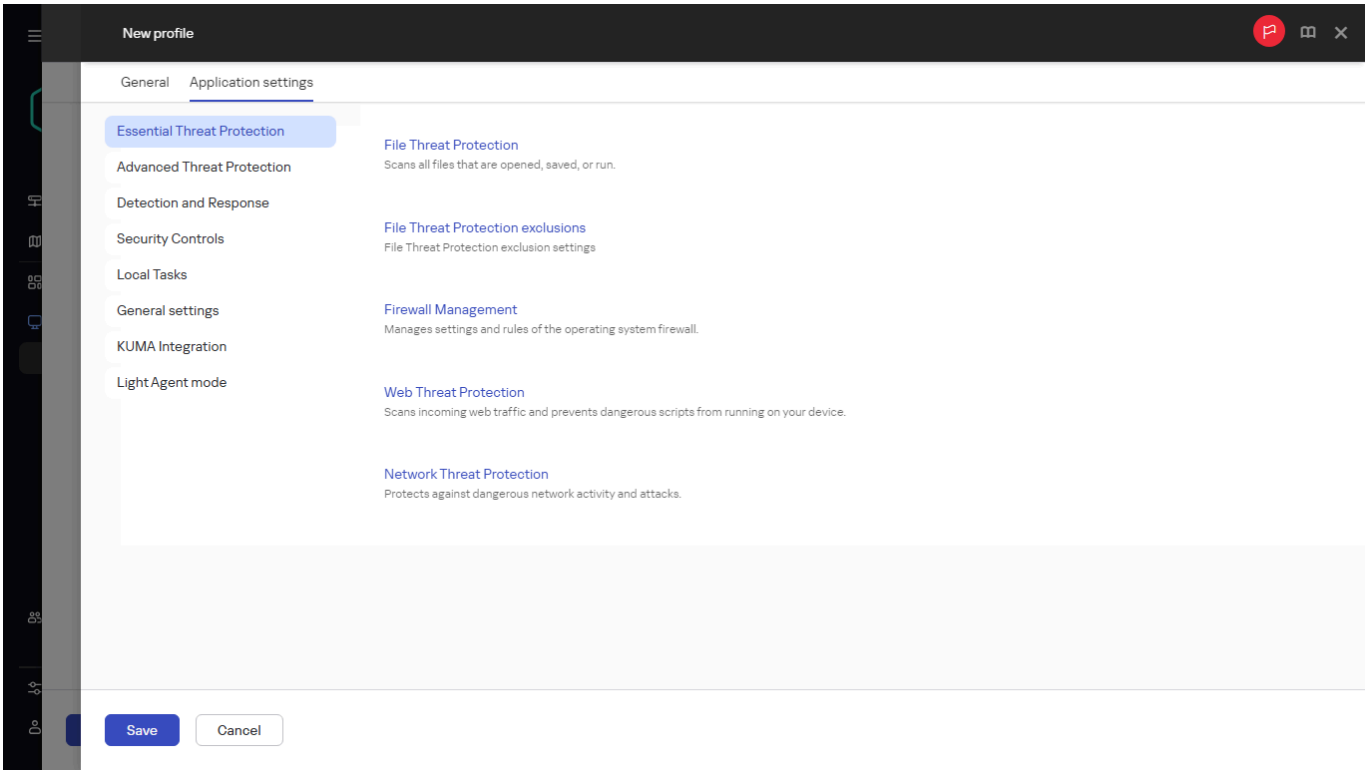
Создание профиля политики

4. Выберите вкладку **Параметры приложения**.

   Можно также нажать на кнопку **Сохранить**, чтобы выйти. Созданный профиль политики отобразится в списке профилей политики, и вы сможете изменить его свойства позже.

5. В левой области вкладки **Параметры приложения** выберите нужный вам раздел и в панели результатов измените параметры профиля политики. Вы можете изменить параметры профиля политики в каждом разделе.

Чтобы отменить изменения, вы можете нажать на кнопку **Отмена**.



Указание параметров профиля политики

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения профиля.

   Профиль политики отобразится в списке профилей политики.

Изменение профиля политики

Изменение профиля доступно только для политик Kaspersky Endpoint Security для Windows.

Чтобы изменить профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На вкладке **Профили политики** нажмите на профиль политики, который вы хотите изменить.

   В результате откроется окно свойств профиля политики.

3. В окне свойств настройте параметры профиля:

   - Если необходимо, на вкладке **Общие** измените имя профиля политики и включите или выключите профиль.
   - Измените правила активации профиля политики.
   - Измените остальные параметры.

Подробнее о параметрах приложений безопасности см. в документации к соответствующему приложению.

4. Нажмите на кнопку **Сохранить**.

Измененные параметры начнут действовать после синхронизации устройства с Сервером администрирования (если профиль политики активен) либо после выполнения правила активации (если профиль политики неактивен).

Копирование профиля политики

Вы можете скопировать профиль политики в текущую политику или в другую политику, например, если вы хотите иметь идентичные профили политик для разных политик. Вы также можете использовать копирование, если хотите иметь два или более профилей политики, которые отличаются небольшим количеством параметров.

Чтобы скопировать профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики. Если у политики нет профилей политики, отобразится пустая таблица.

2. На вкладке **Профили политики** выберите профиль, который требуется скопировать.

3. Нажмите на кнопку **Копировать**.

4. В открывшемся окне выберите политику, в которую требуется скопировать профиль политики.

   Вы можете скопировать профиль политики в эту же политику или в политику, которую вы выбрали.

5. Нажмите на кнопку **Копировать**.

Профиль политики скопирован в политику, которую вы выбрали. Новый скопированный профиль политики имеет самый низкий приоритет. Если вы скопировали профиль политики в эту же политику, к имени такого профиля добавляется окончание вида (<порядковый номер>), например: (1), (2).

Позже вы можете изменить параметры профиля политики, включая его имя и приоритет. В этом случае исходный профиль политики не будет изменен.

Создание правила активации профиля политики

Чтобы создать правило активации профиля политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На вкладке **Профили политики** нажмите на профиль политики, для которого требуется создать правило активации.

   Если список профилей политики пуст, вы можете создать профиль политики.

3. На вкладке **Правила активации** нажмите на кнопку **Добавить**.

   Откроется окно с правилами активации профиля политики.

4. Укажите имя правила активации.

5. Установите флажки напротив условий, которые должны влиять на активацию создаваемого профиля политики:

   Общие правила активации профиля политики

   Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от состояния автономного режима устройства, правила подключения устройства к Серверу администрирования и назначенных устройству тегов.

   Для этого параметра на следующем шаге укажите:

   Статус устройства

   Определяет условие присутствия устройства в сети:

   - **В сети** – устройство находится в сети, Сервер администрирования доступен.
   - **Не в сети** – устройство находится во внешней сети, то есть Сервер администрирования недоступен.
   - **Неизвестно** – критерий не применяется.

   Параметры сетевого местоположения устройства

   Выберите условие для активации профиля политики (независимо от того, выполняется ли это правило или нет) и выберите имя правила.

   Правило определяется сетевым местоположением устройства для подключения к Серверу администрирования, при выполнении или невыполнении условий которого профиль политики будет активирован.

   Описание сетевого местоположения устройств для подключения к Серверу администрирования можно создать или настроить в правиле переключения Агента администрирования.

   - **Правила для выбранного владельца устройства**

     Для этого параметра на следующем шаге укажите:

     Владелец устройства

     Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по владельцу устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

     - устройство принадлежит указанному владельцу (знак "=");
     - устройство не принадлежит указанному владельцу (знак "#").

       Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать владельца устройства, когда параметр включен. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

     Владелец устройства включен во внутреннюю группу безопасности

Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по членству владельца устройства во внутренней группе безопасности Kaspersky SIEM Cloud. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- владелец устройства является членом указанной группы безопасности (знак "=");
- владелец устройства не является членом указанной группы безопасности (знак "#").

  Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать группу безопасности Kaspersky SIEM Cloud. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Правила для характеристик оборудования**

  Установите флажок, чтобы настроить условие активации профиля политики на устройстве в зависимости от объема памяти и количества логических процессоров устройства.

  Для этого параметра на следующем шаге укажите:

  Объем оперативной памяти (МБ)

  Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по объему оперативной памяти устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

  - объем оперативной памяти устройства меньше указанного значения (знак "<");
  - объем оперативной памяти устройства больше указанного значения (знак ">").

  Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать объем оперативной памяти устройства. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

  Количество логических процессоров

  Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по количеству логических процессоров устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

  - количество логических процессоров устройства меньше или равно указанному значению (знак " <");
  - количество логических процессоров устройства больше или равно указанному значению (знак ">").

  Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать количество логических процессоров устройства. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Правила для назначения роли**

  Для этого параметра на следующем шаге укажите:

  Активировать профиль политики по наличию роли у владельца устройства

  Включите этот параметр, чтобы настроить и включить правило активации профиля политики на устройстве в зависимости от наличия определенной роли у его владельца. Добавить роль вручную из списка существующих ролей.

  Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием.

- **Правила для использования тега**

  Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от тегов, назначенных устройству. Вы можете активировать профиль политики либо на устройствах, которые имеют выбранные теги, либо не имеют их.

  Для этого параметра на следующем шаге укажите:

  Список тегов

  В списке тегов задайте правило включения устройств в профиль политики, установив флажки нужным тегам.

  Вы можете добавить в список новые теги, введя их в поле над списком и нажав на кнопку **Добавить**.

  В профиль политики будут включены устройства, в описании которых есть все выбранные теги. Если флажки сняты, критерий не применяется. По умолчанию флажки сняты.

  Применить к устройствам без выбранных тегов

  Включите параметр, если необходимо инвертировать выбор тегов.

  Если параметр включен, в профиль политики будут включены устройства, в описании которых нет выбранных тегов. Если этот параметр выключен, критерий не применяется.

  По умолчанию параметр выключен.

- **Правила для использования Active Directory**

  Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от размещения устройства в подразделении Active Directory или же от членства устройства или его владельца в группе безопасности Active Directory.

  Для этого параметра на следующем шаге укажите:

  Членство владельца устройства в группе безопасности Active Directory

  Если параметр включен, профиль политики активируется на устройстве, владелец которого является членом указанной группы безопасности. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

  Членство устройства в группе безопасности Active Directory

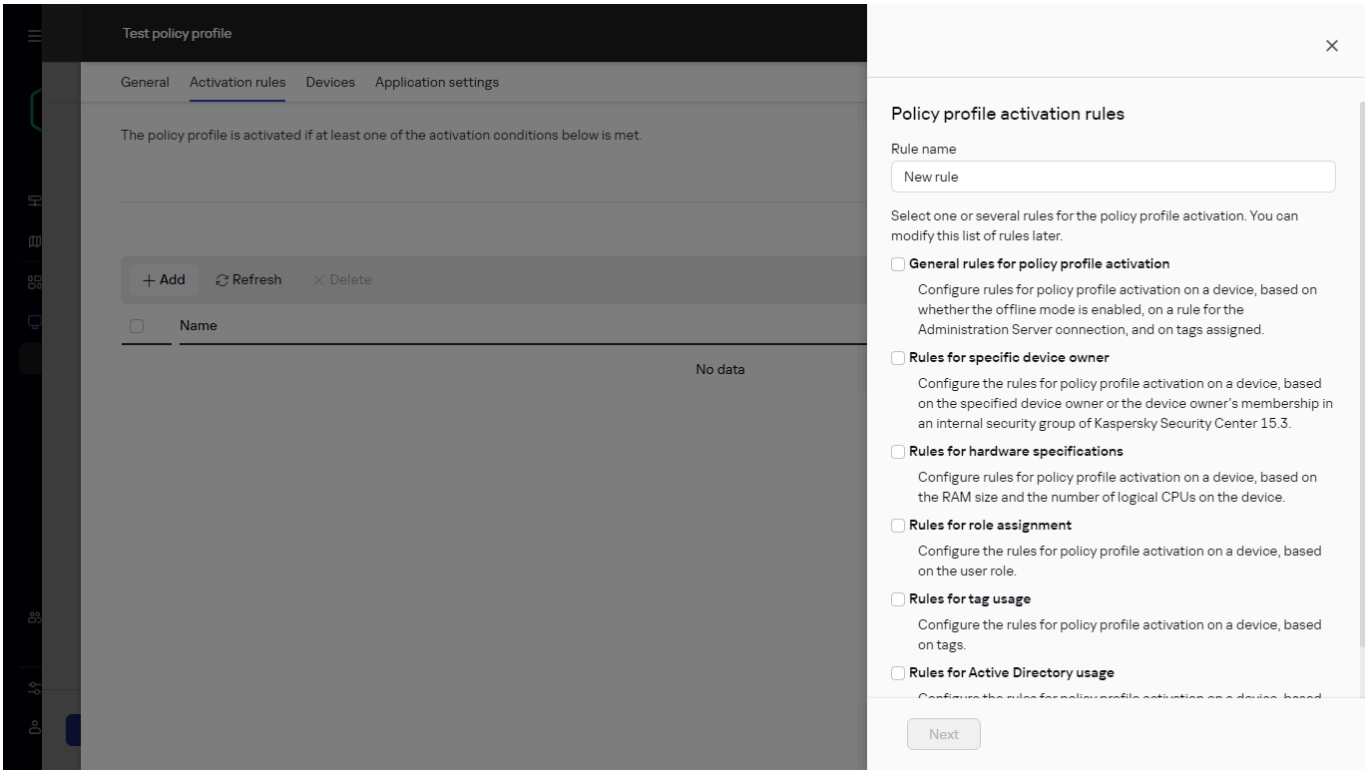
  Если параметр включен, профиль политики активируется на устройстве. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

  Размещение устройства в подразделении Active Directory

  Если параметр включен, профиль политики активируется на устройстве, которое входит в указанное подразделение Active Directory (OU). Если параметр выключен, критерий активации профиля не применяется.

  По умолчанию параметр выключен.

От выбора параметров на этом шаге зависит дальнейшее количество окон мастера. Вы можете изменить правила активации профиля политики позже.



Создание правила активации профиля политики.

6. Проверьте список настроенных параметров. Если список верен, нажмите на кнопку **Создать**.

   В результате профиль будет сохранен. Профиль будет активирован на устройстве, когда будут выполнены правила активации.

Правила активации профиля политики, созданные для профиля, отображаются в свойствах профиля политики на вкладке **Правила активации**. Вы можете изменить или удалить правило активации профиля политики.

Несколько правил активации могут выполняться одновременно.

Удаление профиля политики

Чтобы удалить профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На странице **Профили политики** установите флажок рядом с профилем политики, который вы хотите удалить, и нажмите на кнопку **Удалить**.

3. В появившемся окне нажмите на кнопку **Удалить** еще раз.

   Профиль политики удален. Если политика наследуется группой более низкого уровня, профиль политики остается в этой группе, но становится профилем политики этой группы. Это позволяет уменьшить изменения в параметрах управляемых приложений, установленных на устройствах групп нижнего уровня.

Экспорт и импорт профиля политики

Вы можете сохранить профиль политики в файл KLPROF без экспорта политики, а затем использовать этот файл KLPROF для импорта сохраненного профиля в политику.

Это позволяет быстро восстановить параметры профиля политики вместо их повторной настройки.

Профиль политики импортируется в политику той же версии приложения, из которой вы экспортировали профиль. Для приложений, поддерживающих обратную совместимость политик (например, Kaspersky Endpoint Security for Windows), вы можете импортировать профили политики в разные версии политики.

Чтобы экспортировать профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На вкладке **Профили политики** нажмите на профиль политики, который вы хотите экспортировать.

3. В панели инструментов нажмите на кнопку **Экспортировать**.

4. В открывшемся окне укажите директорию, в которую вы хотите сохранить в файл с профилем политики.

   При необходимости измените имя файла.

5. Нажмите на кнопку **Сохранить**.

Если операция завершена успешно, на экране отобразится соответствующее сообщение. Иначе отобразится сообщение об ошибке.

Чтобы импортировать профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. В панели инструментов нажмите на кнопку **Импортировать**.

3. В открывшемся окне выберите файл KLPROF с нужным профилем политики и нажмите на кнопку **Открыть**.

   Максимальный размер импортируемого файла – 4 МБ.

Если операция завершена успешно, на экране отобразится соответствующее сообщение. Иначе отобразится сообщение об ошибке.

Профиль политики импортируется с именем, которое он имел при экспорте, а не с именем файла KLPROF.
Файл импортируется со статусом **Выключен** и самым низким приоритетом, независимо от приоритета, который был у профиля политики перед экспортом.

Вы не можете выполнить импорт в следующих случаях:

- У политики уже есть профиль с таким же именем.
- Количество профилей в политике равно 100.

Шифрование и защита данных

Шифрование данных снижает риски непреднамеренной утечки информации в случае кражи/утери портативного устройства или жесткого диска, или при доступе к данным неавторизованных пользователей и приложений.

Шифрование поддерживают следующие приложения "Лаборатории Касперского":

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

Вы можете отобразить или скрыть некоторые элементы интерфейса, связанные с управлением шифрованием, с помощью параметров пользовательского интерфейса.

Не рекомендуется включать шифрование в VDI.

Шифрование данных в Kaspersky Endpoint Security for Windows

Вы можете управлять технологией шифрования диска BitLocker на устройствах под управлением операционной системы Windows для серверов или рабочих станций.

С помощью этих компонентов Kaspersky Endpoint Security for Windows вы можете, например, включать или выключать шифрование, просматривать список зашифрованных жестких дисков, формировать и просматривать отчеты о шифровании.

Вы управляете шифрованием, настраивая политики Kaspersky Endpoint Security for Windows в Open Single Management Platform. Kaspersky Endpoint Security for Windows выполняет шифрование и расшифровку в соответствии с активной политикой. Подробные инструкции по настройке правил и описание особенностей шифрования см. в справке Kaspersky Endpoint Security for Windows.

Шифрование данных в Kaspersky Endpoint Security for Mac

Вы можете использовать шифрование FileVault на устройствах с операционными системами macOS. При работе с Kaspersky Endpoint Security for Mac вы можете включить или выключить это шифрование.

Шифрование настраивается путем определения политик Kaspersky Endpoint Security for Mac в Open Single Management Platform. Kaspersky Endpoint Security for Mac выполняет шифрование и расшифровку в соответствии с активной политикой. Подробное описание функций шифрования см. в справке Kaspersky Endpoint Security for Mac.

Просмотр списка зашифрованных жестких дисков

В Open Single Management Platform вы можете просмотреть информацию о зашифрованных жестких дисках и об устройствах, зашифрованных на уровне дисков. После того, как информация на диске будет расшифрована, диск будет автоматически удален из списка.

Чтобы просмотреть список зашифрованных жестких дисков,

В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных** → **Зашифрованные жесткие диски**.

Если раздела нет в меню, значит, он скрыт. В настройках пользовательского интерфейса включите параметр **Показать раздел "Шифрование и защита данных"** для отображения раздела.

Вы можете экспортировать список зашифрованных жестких дисков в файлы форматов CSV или TXT. Для этого нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**.

Формирование и просмотр отчетов о шифровании

Вы можете формировать следующие отчеты:

- Отчет о статусе шифрования управляемых устройств. В этом отчете представлены сведения о шифровании данных различных управляемых устройств. Например, в отчете показано количество устройств, к которым применяется политика с настроенными правилами шифрования. Также можно узнать, например, сколько устройств нужно перезагрузить. Отчет также содержит информацию о технологии и алгоритме шифрования для каждого устройства.

- Отчет о статусе шифрования запоминающих устройств. Этот отчет содержит похожую информацию, что и отчет о состоянии шифрования управляемых устройств, но предоставляет данные только для запоминающих устройств и съемных дисков.

- Отчет о правах доступа к зашифрованным жестким дискам. Этот отчет показывает, какие учетные записи пользователей имеют доступ к зашифрованным жестким дискам.

- Отчет об ошибках шифрования файлов. Отчет содержит информацию об ошибках, которые возникли при выполнении задач шифрования или расшифровки данных на устройствах.

- Отчет о блокировании доступа к зашифрованным файлам. Отчет содержит информацию о блокировке доступа приложений к зашифрованным файлам. Этот отчет полезен, если неавторизованный пользователь или приложение пытается получить доступ к зашифрованным файлам или жестким дискам.

Вы можете сгенерировать любой отчет в разделе **Мониторинг** → **Отчеты**. Также в разделе **Операции** → **Шифрование и защита данных**, можно создавать следующие отчеты о шифровании:

- Отчет о статусе шифрования запоминающих устройств

- Отчет о правах доступа к зашифрованным жестким дискам

- Отчет об ошибках шифрования файлов

*Чтобы сгенерировать отчет шифрования в разделе **Шифрование и защита данных**:*

1. Убедитесь, что параметр **Показать раздел "Шифрование и защита данных"** в параметрах интерфейса включен.
2. В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных**.
3. Откройте раздел **Зашифрованные жесткие диски**, чтобы сформировать отчет о состоянии шифрования запоминающих устройств или отчет о правах доступа к зашифрованным жестким дискам.
4. Выберите название отчета, который требуется сгенерировать.

Запустится процесс формирования отчета.

Предоставление доступа к зашифрованному жесткому диску в автономном режиме

Пользователь может запросить доступ к зашифрованному устройству, например, если Kaspersky Endpoint Security for Windows не установлен на управляемом устройстве. После получения запроса вы можете создать файл ключа доступа и отправить его пользователю. Все варианты использования и подробные инструкции приведены в справке Kaspersky Endpoint Security for Windows.

Чтобы предоставить доступ к зашифрованному жесткому диску в автономном режиме:

1. Получите файл запроса доступа от пользователя (файл с расширением FDERTC). Следуйте инструкциям в справке Kaspersky Endpoint Security for Windows, чтобы сгенерировать файл в Kaspersky Endpoint Security for Windows.
2. В главном окне приложения перейдите в раздел **Операции** → **Шифрование и защита данных** → **Зашифрованные жесткие диски**.

   Отобразится список зашифрованных жестких дисков.
3. Выберите диск, к которому пользователь запросил доступ.
4. Нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.
5. В открывшемся окне выберите плагин, соответствующий приложению "Лаборатории Касперского", которое использовалась для шифрования выбранного диска.
6. Следуйте инструкциям, приведенным в справке Kaspersky Endpoint Security for Windows (см. раскрывающиеся блоки в конце раздела).

После этого пользователь может использовать полученный файл для доступа к зашифрованному жесткому диску и чтения данных, хранящихся на диске.

Передача ключей шифрования между Серверами администрирования

Если на управляемом устройстве включена функция шифрования данных, ключ шифрования хранится на Сервере администрирования. Ключ шифрования используется для доступа к зашифрованным данным и для управления политикой шифрования.

Ключ шифрования должен быть передан на другой Сервер администрирования в следующих случаях:

- Перенастройка Агента администрирования на управляемом устройстве для назначения устройства другому Серверу администрирования. Если это устройство содержит зашифрованные данные, ключ шифрования должен быть передан на целевой Сервер администрирования. В противном случае не удастся расшифровать данные.

- Шифрование съемного диска, подключенного к устройству D1, которым управляет Сервер администрирования S1, и затем подключение этого съемного диска к устройству D2, управляемому Сервером администрирования S2. Для доступа к данным на съемном диске ключ шифрования должен быть передан с Сервера администрирования S1 на Сервер администрирования S2.

- Шифрование файла на устройстве D1, управляемом Сервером администрирования S1, и затем попытка получить доступ к файлу на устройстве D2, управляемом Сервером администрирования S2. Для доступа к файлу ключ шифрования должен быть передан с Сервера администрирования S1 на Сервер администрирования S2.

Ключи шифрования можно передавать следующими способами:

- Автоматически, включив параметр **Использовать иерархию Серверов администрирования для получения ключей шифрования** в свойствах двух Серверов администрирования, между которыми должен передаваться ключ шифрования. Если этот параметр выключен для одного из Серверов администрирования, автоматическая передача ключей шифрования невозможна.

  При включении параметра **Использовать иерархию Серверов администрирования для получения ключей шифрования** в свойствах Сервера администрирования, Сервер администрирования отправляет ключи шифрования на главный Сервер администрирования (если он существует) на один уровень иерархии выше.

  Когда вы пытаетесь получить доступ к зашифрованным данным, Сервер администрирования сначала ищет ключ шифрования в своем хранилище. Если включен параметр **Использовать иерархию Серверов администрирования для получения ключей шифрования**, а требуемый ключ шифрования отсутствует в хранилище, Сервер администрирования дополнительно отправляет запрос на главный Сервер администрирования (если он существует), чтобы получить требуемый ключ шифрования. Запрос отправляется на все главные Серверы администрирования, вплоть до Сервера на самом верхнем уровне иерархии.

- Вручную от одного Сервера администрирования другому путем экспорта и импорта файла, содержащего ключи шифрования.

  Экспорт и импорт ключей шифрования – это действия, включенные в функционал управления ключами шифрования. Чтобы выполнить эти действия, настройте права доступа к функции для пользователей Open Single Management Platform следующим образом:

  - Предоставить право **Чтение** к функции Управление ключами шифрования для пользователя, который экспортирует ключи шифрования с подчиненного Сервера администрирования.

  - Предоставить право **Запись** к функции Управление ключами шифрования для пользователя, импортирующего ключи шифрования на требуемый Сервер администрирования.

Чтобы включить автоматическую передачу ключей шифрования между Серверами администрирования в иерархии:

1. Перейдите в свойства нужного Сервера администрирования:

   a. В главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**.

   b. В открывшейся панели наведите курсор мыши на название нужного Сервера администрирования и нажмите на значок параметров (⚙).

      Вы также можете нажать на имя Сервера администрирования, а после того как имя отобразится в главном меню, нажать на него в главном меню, чтобы открыть окно свойств Сервера.

2. В открывшемся окне свойств выберите раздел **Алгоритм шифрования**.

3. Включите параметр **Использовать иерархию Серверов администрирования для получения ключей шифрования**.

4. Нажмите на кнопку **Сохранить**, чтобы применить изменения.

Ключи шифрования будут переданы на главный Сервер администрирования (если он существует) при следующей синхронизации (пакете пульса). Этот Сервер администрирования также предоставляет по запросу ключ шифрования от своего хранилища подчиненному Серверу администрирования.

Чтобы передать ключи шифрования между Серверами администрирования вручную:

1. Перейдите в свойства Сервера администрирования, с которого вы хотите экспортировать ключи шифрования:

   a. В главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**.

   b. В открывшейся панели наведите курсор мыши на название нужного Сервера администрирования и нажмите на значок параметров (⚙).

      Вы также можете нажать на имя Сервера администрирования, а после того как имя отобразится в главном меню, нажать на него в главном меню, чтобы открыть окно свойств Сервера.

2. В открывшемся окне свойств выберите раздел **Алгоритм шифрования**.

3. Нажмите на кнопку **Экспорт ключей шифрования**.

   Убедитесь, что пользователю, который экспортирует ключи шифрования с Сервера, предоставлено право **Чтение** к функции Управления ключами шифрования.

4. В окне **Экспортировать ключи шифрования с Сервера администрирования?** выполните следующие действия:

   a. Укажите пароль, чтобы защитить файл от несанкционированного доступа.

   b. Укажите, куда сохранить файл.

> Запомните пароль. Утерянный пароль не может быть восстановлен. Если пароль утерян, необходимо повторить процедуру экспорта. Поэтому запишите пароль и держите его под рукой.

5. Передайте файл на другой Сервер администрирования, например, с помощью папки общего доступа или съемного диска.

6. Перейдите в свойства Сервера администрирования, на который вы хотите импортировать ключи шифрования.

7. В окне свойств выберите раздел **Алгоритм шифрования**.

8. Нажмите на кнопку **Импорт ключей шифрования**.

   Убедитесь, что пользователю, импортирующему ключи шифрования на Сервер, предоставлено право **Запись** к функции Управления ключами шифрования.

9. Выберите файл, содержащий ключи шифрования.

10. Укажите пароль и нажмите на кнопку **OK**.

Ключи шифрования будут переданы на целевой Сервер администрирования.

Управление пользователями и ролями пользователей

В этом разделе описана работа с пользователями и ролями пользователей, а также приведены инструкции по их созданию и изменению, назначению пользователям ролей и групп и связи профилей политики с ролями.

Об учетных записях пользователей

Kaspersky SIEM Cloud позволяет управлять учетными записями пользователей и группами учетных записей. Приложение поддерживает три типа учетных записей:

- Учетные записи сотрудников организации. Сервер администрирования получает данные об учетных записях этих доменных пользователей при опросе контроллеров доменов организации.
- Учетные записи локальных пользователей. Локальные учетные записи управляемых устройств, а также локальные учетные записи устройства, на котором установлен Сервер администрирования.
- Учетные записи внутренних пользователей Kaspersky SIEM Cloud. Вы можете создавать учетные записи внутренних пользователей. Эти учетные записи используются только в Kaspersky SIEM Cloud.

В Kaspersky SIEM Cloud вы можете добавить не более 17 000 учетных записей пользователей.

Чтобы просмотреть таблицы учетных записей пользователей и групп безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы**.

2. Выберите вкладку **Пользователи** или **Группы**.

Откроется таблица пользователей или групп безопасности. По умолчанию открытая таблица фильтруется по столбцам **Тип учетной записи** и **Имеет назначенные роли**. В таблице показаны внутренние пользователи или группы, которым назначены роли.

Если вы хотите просмотреть таблицу только с учетными записями локальных пользователей, установите в фильтре **Тип учетной записи** критерий **Локальный**.

Если вы переключитесь на подчиненный Сервер администрирования версии 14.2 или ниже, а затем откроете список пользователей или групп безопасности, то открытая таблица будет отфильтрована только по столбцу **Тип учетной записи**. Фильтр по столбцу **Имеет назначенные роли** не будет применяться по умолчанию. Отфильтрованная таблица будет содержать всех внутренних пользователей или группы безопасности с назначенной ролью и без нее.

Добавление учетной записи внутреннего пользователя

В Kaspersky Security Center Cloud Console вы можете добавлять новых пользователей в рабочую область. Например, вы можете назначить добавленного пользователя владельцем устройства.

В Kaspersky SIEM Cloud вы можете добавить не более 17 000 учетных записей пользователей.

Чтобы добавить учетную запись внутреннего пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы**.
2. На вкладке **Пользователи** нажмите **Добавить**.
3. В открывшемся окне **Добавить пользователей** введите адрес электронной почты пользователя, которого вы хотите добавить, и нажмите на кнопку **Далее**.
4. Просмотрите и измените данные пользователя.
5. Нажмите на кнопку **Готово**, чтобы сохранить изменения.

Учетная запись внутреннего пользователя будет добавлена и появится в списке пользователей.

Чтобы изменить информацию учетной записи внутреннего пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы**.
2. В списке пользователей нажмите на учетную запись пользователя, которую требуется изменить.
3. В открывшемся окне измените необходимую информацию.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Чтобы разрешить добавленному внутреннему пользователю входить в Web Console и управлять рабочей областью, вы можете предоставить ему права администратора рабочей области в Kaspersky Security Center Cloud Console. Вы также можете удалить учетную запись внутреннего пользователя.

Удаление учетной записи внутреннего пользователя

Чтобы удалить учетную запись внутреннего пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы**.
2. Установите флажок напротив пользователя, которого нужно удалить.
3. Нажмите на кнопку **Удалить**.
4. Подтвердите удаление.

Учетная запись внутреннего пользователя удалена и не может быть восстановлена.

Назначение администраторов рабочей области

В Kaspersky Security Center Cloud Console вы можете предоставить пользователям права администратора рабочей области. Администраторы рабочей области могут войти в Web Console и управлять рабочей областью.

Чтобы назначить администратора рабочей области:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы**.
2. На вкладке **Пользователи** нажмите на имя пользователя, которого вы хотите назначить администратором рабочей области.
3. В открывшемся окне включите переключатель **Администратор рабочей области**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Чтобы отозвать права администратора рабочей области, выключите переключатель **Администратор рабочей области**.

О ролях пользователей

Роль пользователя (далее также *роль*) это объект, содержащий набор прав и разрешений. Роль может быть связана с параметрами приложениями "Лаборатории Касперского", которые установлены на устройстве пользователя. Вы можете назначить роль набору пользователей или набору групп безопасности на любом уровне иерархии групп администрирования, Серверов администрирования либо на уровне конкретных объектов.

Если вы управляете устройствами с помощью иерархии Серверов администрирования, в которую входят виртуальные Серверы администрирования, обратите внимание, что вы можете создавать, изменять и удалять пользовательские роли только на физическом Сервере администрирования. Затем вы можете распространить пользовательские роли на подчиненные Серверы администрирования, в том числе виртуальные Серверы.

Вы можете связывать роли с профилями политик. Если пользователю назначена роль, этот пользователь получает параметры безопасности, требуемые для выполнения служебных обязанностей.

Роль пользователя может быть связана с устройствами пользователей заданной группы администрирования.

Область роли пользователя

Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Преимущество использования ролей

Преимущество использования ролей заключается в том, что вам не нужно указывать параметры безопасности для каждого управляемого устройства или для каждого из пользователей отдельно. Количество пользователей и устройств в компании может быть большим, но количество различных служебных обязанностей, требующих разных параметров безопасности, значительно меньше.

Отличия от использования профилей политики

Профили политики – это свойства политики, созданной для каждого приложения "Лаборатории Касперского" отдельно. Роль связана со многими профилями политики, которые созданы для разных приложений. Таким образом, роль – это метод объединения параметров для определенного типа пользователя.

Настройка прав доступа к функциям приложения. Управление доступом на основе ролей

Kaspersky SIEM Cloud предоставляет доступ на основе ролей к функциям Kaspersky SIEM Cloud и к функциям управляемых приложений "Лаборатории Касперского".

Вы можете настроить права доступа к функциям приложения для пользователей Kaspersky SIEM Cloud одним из следующих способов:

- настраивать права каждого пользователя или группы пользователей индивидуально;
- создавать типовые роли пользователей с заранее настроенным набором прав и присваивать роли пользователям в зависимости от их служебных обязанностей.

Применение ролей пользователей облегчает и сокращает рутинные действия по настройке прав доступа пользователей к приложению. Права доступа в роли настраивают в соответствии с типовыми задачами и служебными обязанностями пользователей.

Ролям пользователя можно давать названия, соответствующие их назначению. В приложение можно создавать неограниченное количество ролей.

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли и самостоятельно настраивать необходимые права.

Права доступа к функциям приложения

В таблице ниже приведены функции Kaspersky SIEM Cloud с правами доступа для управления задачами, отчетами, параметрами и для выполнения действий пользователя.

Для выполнения действий пользователя, перечисленных в таблице, у пользователя должно быть право, указанное рядом с действием.

Права на **Чтение**, **Запись** и **Выполнение** применимы к любой задаче, отчету или параметрам. В дополнение к этим правам у пользователя должно быть право **Выполнение операций с выборками устройств** для управления задачами, отчетами или изменения параметров выборок устройств.

> Все задачи, отчеты, параметры и инсталляционные пакеты, отсутствующие в таблице, относятся к области **Общие функции: Базовая функциональность**.

Права доступа к функциям приложения

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
Общие функции: **Управление группами администрирования**	**Запись.**	• Добавление устройства в группу администрирования: **Запись**. • Удаление устройства из состава группы администрирования: **Запись**. • Добавление группы администрирования в другую группу администрирования: **Запись**. • Удаление группы администрирования из другой группы администрирования: **Запись**.	Отсутствует.	Отсутствует.	Отс

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
Общие функции: **Доступ к объектам независимо от их списков ACL**	**Чтение.**	Получение доступа на чтение ко всем объектам: **Чтение**.	Отсутствует.	Отсутствует.	Фун обла **фун объ неза спи** пред ауди поль пред прав фун обла полу дост всем Реко пред прав круг кото для слу обя: Дос пред неза прав запр чте опр объ
Общие функции: **Базовая функциональность**.	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Правила перемещения устройства (создание, изменение или удаление) для виртуального Сервера: **Запись**, **Выполнение действий над выборками устройств**. • Получение мобильного протокола (LWNGT) пользовательского сертификата: **Чтение**. • Установка мобильного протокола (LWNGT) пользовательского сертификата: **Запись**. • Получить список сетей, определенных NLA: **Чтение**. • Добавить, изменить или удалить список сетей, определенных NLA: **Запись**. • Просмотр списка контроля доступа групп: **Чтение**. • Просмотрите журнал событий Kaspersky Event Log: **Чтение**.	• Загрузка обновлений в хранилище Сервера администрирования. • Рассылка отчетов. • Распространение инсталляционных пакетов. • Установка приложений на подчиненные Серверы администрирования.	• Отчет о состоянии защиты. • Отчет об угрозах. • Отчет о наиболее заражаемых устройствах. • Отчет о статусе антивирусных баз. • Отчет об ошибках. • Отчет о сетевых атаках. • Сводный отчет о приложениях для защиты почтовых систем. • Сводный отчет о приложениях для защиты периметра. • Сводный отчет о типах установленных приложений. • Отчет о пользователях зараженных устройств. • Отчет о проблемах безопасности. • Отчет о событиях. • Отчет о работе точек распространения. • Отчет о подчиненных Серверах администрирования. • Отчет о событиях Контроля устройств. • Отчет об уязвимостях.	Отс

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
				• Отчет о запрещенных приложениях. • Отчет о работе Веб-Контроля. • Отчет о статусе шифрования управляемых устройств. • Отчет о статусе шифрования запоминающих устройств. • Отчет об ошибках шифрования файлов. • Отчет о блокировании доступа к зашифрованным файлам. • Отчет о правах доступа к зашифрованным устройствам. • Отчет об эффективных правах пользователя. • Отчет о правах.	
Общие функции: **Удаленные объекты**	• **Чтение.** • **Запись.**	• Просмотр удаленных объектов в корзине: **Чтение**. • Удаление объектов из корзины: **Запись**.	Отсутствует.	Отсутствует.	Отс
Общие функции: **Обработка событий**	• **Удаление событий.** • **Изменение параметров уведомления о событиях.** • **Изменение параметров записи событий в журнал событий.** • **Запись.**	• Изменение параметров регистрации событий: **Изменение параметров записи событий в журнал событий**. • Изменение параметров уведомления о событиях: **Изменение параметров уведомления о событиях**. • Удаление событий: **Удаление событий**.	Отсутствует.	Отсутствует.	Пар • • • •
Общие функции: **Развертывание приложений "Лаборатории Касперского"**	• **Управление патчами "Лаборатории Касперского".** • **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	Одобрить или отклонить установку патча: **Управление патчами "Лаборатории Касперского"**.	Отсутствует.	• Отчет об использовании лицензионных ключей виртуальным Сервером администрирования. • Отчет о версиях приложений "Лаборатории Касперского".	Инс паке "Лаб Кас

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
				• Отчет о несовместимых приложениях. • Отчет о версиях обновлений модулей приложений "Лаборатории Касперского". • Отчет о развертывании защиты.	
Общие функции: **Управление лицензионными ключами**	• **Экспорт файл ключа.** • **Запись.**	• Экспорт файл ключа: **Экспорт файл ключа.** • Изменение параметров лицензионного ключа Сервера администрирования: **Запись**.	Отсутствует.	Отсутствует.	Отс
Общие функции: **Управление отчетами**	• **Чтение.** • **Запись.**	• Создание отчетов для объектов независимо от их списков ACL: **Запись**. • Выполнять отчеты независимо от их списков ACLs: **Чтение**.	Отсутствует.	Отсутствует.	Отс

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
Общие функции: **Иерархия Серверов администрирования**	**Настройка иерархии Серверов администрирования**	Добавление, обновление или удаление подчиненных Серверов администрирования: **Настройка иерархии Серверов администрирования**.	Отсутствует.	Отсутствует.	Отс
Общие функции: **Права пользователя**	**Изменение списков ACL объекта.**	• Изменение свойств Безопасности любого объекта: **Изменение списков ACL объекта**. • Управление ролями пользователей: **Изменение списков ACL объекта**. • Управление внутренними пользователями: **Изменение списков ACL объекта**. • Управление группами безопасности: **Изменение списков ACL объекта**. • Управление псевдонимами: **Изменение списков ACL объекта**.	Отсутствует.	Отсутствует.	Отс
Общие функции: **Виртуальные Серверы администрирования**	• **Управление виртуальными Серверами администрирования.** • **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Получение списка виртуальных Серверов администрирования: **Чтение**. • Получение информации о виртуальном Сервере администрирования: **Чтение**. • Создание, обновление или удаление виртуального Сервера администрирования: **Управление виртуальными Серверами администрирования**. • Перемещение виртуального Сервера администрирования в другую группу: **Управление виртуальными Серверами администрирования**. • Установка прав доступа к виртуальному Серверу администрирования: **Управление виртуальными Серверами администрирования**.	Отсутствует.	Отчет о результатах установки обновлений стороннего ПО.	Отс

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
Общие функции: Управление ключами шифрования	**Запись.**	Импорт ключей шифрования: **Запись**.	Отсутствует.	Отсутствует.	Отс
Управление системой: **Подключения**	• **Запуск RDP-сеансов.** • **Подключение к существующим RDP-сеансам.** • **Туннелирование.** • **Сохранение файлов с устройств на рабочем месте администратора.** • **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Создание сеанса совместного доступа к рабочему столу: **Право на создание сеанса совместного доступа к рабочему столу**. • Создание RDP-сеанса: **Подключение к существующим RDP-сеансам**. • Создание туннеля: **Туннелирование**. • Сохранение списка сетей: **Сохранение файлов с устройств на рабочем месте администратора**.	Отсутствует.	Отчет о пользователях устройства.	Отс
Управление системой: **Инвентаризация оборудования**	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Получение или экспорт объектов инвентаризации оборудования: **Чтение**. • Добавление, установка или удаление объектов инвентаризации оборудования: **Запись**.	Отсутствует.	• Отчет о реестре оборудования. • Отчет об изменении конфигурации. • Отчет об оборудовании.	Отс
Управление системой: **Управление доступом в сеть**	• **Чтение.** • **Запись.**	• Просмотр параметров Cisco: **Чтение**. • Изменение параметров Cisco: **Запись**.	Отсутствует.	Отсутствует.	Отс
Управление системой: **Развертывание операционной системы**	• **Развертывание PXE-серверов.** • **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Развертывание PXE-серверов: **Развертывание PXE-серверов**. • Просмотр списка PXE-серверов: **Чтение**. • Запуск или остановка процесс установки на PXE-клиентах: **Выполнение**. • Управление драйверами для среды WinPE и образов операционной системы: **Запись**.	Создание инсталляционного пакета на основе образа ОС эталонного устройства.	Отсутствует.	Инст паке опер сист
Управление системой: **Системное администрирование**	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Просмотр свойства патчей сторонних производителей: **Чтение**. • Изменение свойства патчей сторонних производителей: **Запись**.	• Выполнение синхронизации обновлений Центра обновления Windows. • Установка обновлений Центра обновления Windows.	Отчет об обновлениях ПО.	Отс

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	
			• Закрытие уязвимостей. • Установка требуемых обновлений и закрытия уязвимостей.		
Управление системой: **Удаленная установка**	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Просмотр Системного администрирования стороннего производителя на основе свойств инсталляционного пакета: **Чтение**. • Изменение Системного администрирования на основе свойств инсталляционного пакета: **Запись**.	Отсутствует.	Отсутствует.	Инст паке • •
Управление системой: **Инвентаризация приложений**	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	Отсутствует.	Отсутствует.	• Отчет об установленных приложениях. • Отчет об истории реестра приложений. • Отчет о состоянии групп лицензионных приложений. • Отчет о лицензионных ключах сторонних приложений.	Отс

Предопределенные роли пользователей

Роли пользователей, назначенные пользователям Kaspersky SIEM Cloud, предоставляют им набор прав доступа к функциям приложения.

Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли. При создании роли вам нужно задать область действия и назначить права доступа к функциям Open Single Management Platform. Некоторые из предопределенных пользовательских ролей, доступных в Kaspersky SIEM Cloud, можно связать с определенными должностями, например, **Аудитор**, **Специалист по безопасности**, **Контролер**. Права доступа этих ролей предварительно настраиваются в соответствии со стандартными задачами и обязанностями соответствующих должностей. В таблице ниже показано как роли могут быть связаны с определенными должностями.

Примеры ролей для определенных должностей

Роль	Комментарий
Аудитор	Разрешены все операции по просмотру и выполнению любых созданных задач на выбранных устройствах, подключенных к Серверу администрирования через Агент администрирования с правами локального администратора (с правами root для Linux). Рекомендуется предоставлять эти права ограниченному количеству пользователей, которым они нужны для выполнения своих служебных обязанностей.

Контролер	Разрешен просмотр всех операций, не разрешены другие операции. Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации.
Специалист по безопасности	Разрешены всех операции просмотра, разрешено управление отчетами; предоставлены ограниченные права в области **Управление системой**: **Подключения**. Вы можете назначить эту роль сотруднику, который отвечает за IT-безопасность в вашей организации.

В таблице ниже приведены права для каждой предопределенной роли пользователя.

Права предопределенных ролей пользователей

Роль	Описание

Администратор Сервера администрирования	Разрешает все операции в следующих функциональных областях:
	• **Общие функции**:
	  • **Базовая функциональность.**
	  • **Управление ключами шифрования.**
	  • **Обработка событий.**
	  • **Иерархия Серверов администрирования.**
	  • **Виртуальные Серверы администрирования.**
	• **Управление системой**:
	  • **Подключения.**
	  • **Инвентаризация оборудования.**
	  • **Инвентаризация приложений.**

Оператор Сервера администрирования	Предоставляет права на **Чтение** и **Выполнение** (если применимо) во всех следующих функциональных областях:
	• **Общие функции**:
	  • **Базовая функциональность.**
	  • **Управление ключами шифрования.**
	  • **Виртуальные Серверы администрирования.**
	• **Управление системой**:
	  • **Подключения.**
	  • **Инвентаризация оборудования.**
	  • **Инвентаризация приложений.**

Аудитор	Разрешает все операции в следующих функциональных областях: **Общие функции**: • **Доступ к объектам независимо от их списков ACL.** • **Удаленные объекты.** • **Управление отчетами.** Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации.

Администратор установки приложений	Разрешает все операции в следующих функциональных областях:
	• **Общие функции:**
	  • **Базовая функциональность.**
	  • **Приложения "Лаборатории Касперского".**
	  • **Управление лицензионными ключами.**
	• **Управление системой:**
	  • **Развертывание операционной системы.**
	  • **Системное администрирование.**
	  • **Удаленная установка.**
	  • **Инвентаризация приложений.**
	Предоставляет права на **Чтение** и **Выполнение** в следующей функциональной области **Базовая функциональность: Виртуальные Серверы администрирования**.

Роль	Описание

Оператор установки приложений	Предоставляет права на **Чтение** и **Выполнение** (если применимо) во всех следующих функциональных областях:
	• **Общие функции:**
	  • **Базовая функциональность.**
	  • **Развертывание приложений "Лаборатории Касперского"** (также предоставляет права на **Управление патчами "Лаборатории Касперского"** в этой же области).
	  • **Виртуальные Серверы администрирования.**
	• **Управление системой:**
	  • **Развертывание операционной системы.**
	  • **Системное администрирование.**
	  • **Удаленная установка.**
	  • **Инвентаризация приложений.**

Администратор Kaspersky Endpoint Security	Разрешает все операции в следующих функциональных областях: • **Общие функции: Базовая функциональность.** • **Общие функции: Управление ключами шифрования.** • Область **Kaspersky Endpoint Security**, включая все функции.
Оператор Kaspersky Endpoint Security	Предоставляет права на **Чтение** и **Выполнение** (если применимо) во всех следующих функциональных областях: • **Общие функции: Базовая функциональность.** • **Общие функции: Управление ключами шифрования.** • Область **Kaspersky Endpoint Security**, включая все функции.
Главный администратор	Разрешает все операции в функциональных областях, *за исключением* следующих областей: **Общие функции**: • **Доступ к объектам независимо от их списков ACL.** • **Управление отчетами.**

Главный оператор	Предоставляет права на **Чтение** и **Выполнение** (если применимо) во всех следующих функциональных областях:
	• **Общие функции**:
	  • **Базовая функциональность.**
	  • **Удаленные объекты.**
	  • **Управление ключами шифрования.**
	  • **Операции с Сервером администрирования.**
	  • **Теги устройств.**
	  • **Приложения "Лаборатории Касперского".**
	  • **Интеграция приложений.**
	  • **Виртуальные Серверы администрирования.**
	• Функциональная область **Управление мобильными устройствами**, включая все функции.
	• Функциональная область **Управление системой**, включая все функции.
	• Область **Kaspersky Endpoint Security**, включая все функции.

Администратор управления мобильными устройствами	Разрешает все операции в следующих функциональных областях: • **Общие функции: Базовая функциональность.** • Функциональная область **Управление мобильными устройствами**, включая все функции. Предоставляет право **Экспортировать файл ключа** в области **Общие функции: Управление лицензионными ключами**. Предоставляет право на **Чтение** в области **Управление системой: Системное администрирование**.
Оператор управления мобильными устройствами	Предоставляет права на **Чтение** и **Выполнение** в области **Общие функции: Базовая функциональность**. Предоставляет права на **Чтение** и **Отправка только информационных команд на мобильные устройства** в области **Управление мобильными устройствами**: • **Общие.** • **Self Service Portal.**

Роль	Описание
Специалист по безопасности	Разрешает все операции в следующих функциональных областях: **Общие функции**: • **Доступ к объектам независимо от их списков ACL.** • **Управление отчетами.** Предоставляет следующие права в функциональной области **Управления системой: Подключения**: **Чтение**, **Запись**, **Выполнение**, **Сохранение файлов с устройств на рабочем месте администратора** и **Выполнение операций с выборками устройств**. Вы можете назначить эту роль сотруднику, который отвечает за IT-безопасность в вашей организации.
Пользователь Self Service Portal	Разрешает все операции в области **Управление мобильными устройствами: Self Service Portal**.
Контролер	Предоставляет права на **Чтение** в области **Общие функции**: **Доступ к объектам независимо от их списков ACL** и **Общие функции**: функциональная область **Управление отчетами**. Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации.
Администратор Системного администрирования	Разрешает все операции в области **Общие функции**: **Базовая функциональность** и **Управление системой** (включая все функции, *кроме* области **Удаленное выполнение скриптов**).
Оператор Системного администрирования	Предоставляет права на **Чтение** и **Выполнение** (если применимо) в области **Общие функции**: **Базовая функциональность** и **Управление системой** (включая все функции, *кроме* области **Удаленное выполнение скриптов**).

Роли XDR

Права предопределенных ролей пользователей функциональных областей XDR

Роль	Описание
Главный администратор	Разрешает все операции в функциональных областях XDR: • **Алерты и инциденты** • **Detection and response** • **Плейбуки и действия по реагированию** • **Управление активами** • **IAM** • **Тенанты** • **Интеграция с приложениями "Лаборатории Касперского"** • **Интеграция с приложениями сторонних производителей** • **Лицензии**
Администратор тенанта	Разрешает все операции в функциональных областях XDR: • **Алерты и инциденты** • **Detection and response** • **Плейбуки и действия по реагированию** • **Управление активами** • **IAM** • **Тенанты** • **Интеграция с приложениями "Лаборатории Касперского"** • **Интеграция с приложениями сторонних производителей** • **Лицензии** Эта роль соответствует роли Главного администратора, но имеет ограничение. В Kaspersky SIEM Cloud администратор тенанта имеет ограниченный доступ к предустановленным объектам.
Администратор SOC	Предоставляет следующие права в функциональных областях XDR: • **Detection and response**: **Чтение, Запись** • **Плейбуки и действия по реагированию**: **Чтение**, **Запись, Удаление** • **IAM**: **Чтение пользователей и ролей**, **Назначение ролей** и **Списки пользователей** • **Тенанты**: **Чтение**, **Запись** • **Интеграция с приложениями "Лаборатории Касперского"**: **Чтение**, **Запись** • **Интеграция с приложениями сторонних производителей**: **Чтение**, **Запись** • **Лицензии**: **Чтение** • **Управление активами: Чтение, Запись, Удаление**

Младший аналитик	Предоставляет следующие права в функциональных областях XDR: • **Алерты и инциденты**: **Чтение** и **Запись** • **Detection and response**: **Чтение** • **Управление активами**: **Чтение** Просмотр сведений • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей** • **Тенанты**: **Чтение** • **Интеграция с приложениями "Лаборатории Касперского"**: **Чтение** • **Интеграция с приложениями сторонних производителей**: **Чтение** • **Лицензии**: **Чтение**
Аналитик 2-го уровня	Предоставляет следующие права в функциональных областях XDR: • **Алерты и инциденты**: **Чтение** и **Запись** • **Detection and response**: **Чтение** • **Плейбуки и действия по реагированию**: **Чтение**, **Запись** и **Выполнение** • **Управление активами** • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей** • **Тенанты**: **Чтение** • **Интеграция с приложениями "Лаборатории Касперского"**: **Чтение** • **Интеграция с приложениями сторонних производителей**: **Чтение** • **Лицензии**: **Чтение**
Аналитик 1-го уровня	Предоставляет следующие права в функциональных областях XDR: • **Алерты и инциденты**: **Чтение** и **Запись**. • **Detection and response**: **Чтение**. • **Плейбуки и действия по реагированию**: **Чтение**, **Запись** и **Выполнение**. • **Управление активами.** • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей**. • **Тенанты**: **Чтение**. • **Интеграция с приложениями "Лаборатории Касперского"**: **Чтение**. • **Интеграция с приложениями сторонних производителей**: **Чтение**. • **Лицензии**: **Чтение**. Эта роль соответствует роли Аналитик 2-го уровня, но она имеет ограничение. В Kaspersky SIEM Cloud аналитик 1-го уровня может изменять только свои собственные объекты.
Менеджер SOC	Предоставляет следующие права в функциональных областях XDR: • **Алерты и инциденты**: **Чтение** и **Запись**. • **Detection and response**: **Чтение**. • **Плейбуки и действия по реагированию**: **Чтение**. • **Управление активами**: **Чтение**. Просмотр сведений • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей**. • **Тенанты**: **Чтение**. • **Интеграция с приложениями "Лаборатории Касперского"**: **Чтение**. • **Интеграция с приложениями сторонних производителей**: **Чтение**. • **Лицензии**: **Чтение**.
Подтверждающий	Предоставляет следующие права в функциональных областях XDR: • **Алерты и инциденты**: **Чтение, Запись, Закрытие**. • **Detection and response**: **Чтение**. • **Плейбуки и действия по реагированию**: **Чтение** и **Подтверждение действий по реагированию**. • **Управление активами**: **Чтение**. Просмотр сведений • **IAM**: **Чтение пользователей и ролей**. • **Тенанты**: **Чтение**. • **Интеграция с приложениями "Лаборатории Касперского"**: **Чтение**. • **Интеграция с приложениями сторонних производителей**: **Чтение**. • **Лицензии**: **Чтение**.
Аудитор	Предоставляет следующие права в функциональных областях XDR: • **Алерты и инциденты**: **Чтение**. • **Detection and response**: **Чтение**. • **Плейбуки и действия по реагированию**: **Чтение**. • **Управление активами**: **Чтение**. Просмотр сведений • **IAM**: **Чтение пользователей и ролей** и **Списки пользователей**. • **Тенанты**: **Чтение**. • **Интеграция с приложениями "Лаборатории Касперского"**: **Чтение**. • **Интеграция с приложениями сторонних производителей**: **Чтение**. • **Лицензии**: **Чтение**.

Взаимодействие с дочерними инцидентами	Предоставляет следующие права в функциональных областях XDR: • **Дочерние инциденты**: **Чтение** и **Запись**. • **IAM**: **Чтение пользователей и ролей**. В дополнение к этой роли у пользователя должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 2-го уровня, Аналитик 1-го уровня, Менеджер SOC, Подтверждающий, Аудитор.
Редактирование общих ресурсов	Предоставляет право изменять доступ к общим ресурсам, расположенным в общем тенанте. В дополнение к этой роли у пользователя должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 2-го уровня, Аналитик 1-го уровня, Менеджер SOC, Подтверждающий.
Чтение общих ресурсов	Предоставляет право на чтение общих ресурсов, расположенных в общем тенанте. В дополнение к этой роли у пользователя должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 2-го уровня, Аналитик 1-го уровня, Менеджер SOC, Подтверждающий.
Управление SLA	Предоставляет право изменять оставшееся время SLA для инцидентов. В дополнение к этой роли у пользователя должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 2-го уровня, Аналитик 1-го уровня, Менеджер SOC, Подтверждающий.
Просмотр универсального макета панели мониторинга	Предоставляет права доступа к просмотру универсального макета панели мониторинга. В дополнение к этой роли у пользователя должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 2-го уровня, Аналитик 1-го уровня, Менеджер SOC, Подтверждающий.
Роли служб	
Автоматическое реагирование на угрозы	Предоставляет учетным записям служб право реагировать на угрозы. Права доступа настраиваются автоматически в соответствии с правами доступа на основе ролей политик Kaspersky Security Center Linux и управляемых приложений "Лаборатории Касперского". Вы можете назначать эту роль только учетным записям служб. Эту роль невозможно изменить.

Роли служб

Права предопределенных ролей для учетных записей служб

Роль	Описание
Автоматическое реагирование на угрозы	Предоставляет учетным записям служб право реагировать на угрозы. Права доступа настраиваются автоматически в соответствии с правами доступа на основе ролей политик Kaspersky Security Center Linux и управляемых приложений "Лаборатории Касперского". Вы можете назначать эту роль только учетным записям служб. Эту роль невозможно изменить.

Назначение прав доступа к набору объектов

В дополнение к назначению прав доступа на уровне сервера, вы можете настроить доступ к конкретным объектам, например, к требуемой задаче. Приложение позволяет указать права доступа к следующим типам объектов:

- Группы администрирования
- Задачи
- Отчеты
- Выборки устройств
- Выборки событий

Чтобы назначить права доступа к конкретному объекту:

1. В зависимости от типа объекта в главном меню перейдите в соответствующий раздел:
   - **Управление активами → Иерархия групп**.
   - **Задачи**.
   - **Мониторинг → Отчеты**.
   - **Управление активами → Выборки устройств**.
   - **Мониторинг → Выборки событий**.
2. Откройте свойства объекта, к которому вы хотите настроить права доступа.

   Чтобы открыть окно свойств группы администрирования или задачи, нажмите на название объекта. Свойства других объектов можно открыть с помощью кнопки в панели инструментов.
3. В окне свойств откройте раздел **Права доступа**.

   Откроется список пользователей. Перечисленные пользователи и группы безопасности имеют права доступа к объекту. Если вы используете иерархию групп администрирования или Серверов, список и права доступа по умолчанию наследуются от родительской группы администрирования или главного Сервера.
4. Чтобы иметь возможность изменять список, включите параметр **Использовать права пользователей**.

5. Настройте права доступа:

   - Используйте кнопки **Добавить** и **Удалить** для изменения списка.
   - Укажите права доступа для пользователя или группы безопасности. Выполните одно из следующих действий:
     - Если вы хотите указать права доступа вручную, выберите пользователя или группу безопасности, нажмите на кнопку **Права доступа** и укажите права доступа.
     - Если вы хотите назначить пользовательскую роль пользователю или группе безопасности, выберите пользователя или группу безопасности, нажмите на кнопку **Роли** и выберите роль для назначения.

6. Нажмите на кнопку **Сохранить**.

Права доступа к объекту настроены.

Назначение прав пользователям или группам безопасности

Вы можете назначить права доступа пользователям или группам безопасности, чтобы использовать различные возможности Сервера администрирования, например Kaspersky Endpoint Security for Linux.

Чтобы назначить права доступа пользователю или группе безопасности:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Права доступа** установите флажок рядом с именем пользователя или группы безопасности, которым нужно назначить права, а затем нажмите на кнопку **Права доступа**.

   Вы не можете выбрать несколько пользователей или групп безопасности одновременно. Если вы выберете более одного объекта, кнопка **Права доступа** будет неактивна.

3. Настройте набор прав для пользователя или группы:

   a. Разверните узел с функциями Сервера администрирования или другого приложения "Лаборатории Касперского".

   b. Установите флажок **Разрешить** или **Запретить** рядом с нужной функцией или правом доступа.

      Пример 1: Установите флажок **Разрешить** рядом с узлом **Интеграции приложения**, чтобы предоставить пользователю или группе все доступные права доступа к функции интеграции приложения (**Чтение**, **Запись** и **Выполнение**).

      Пример 2: Разверните узел **Управление ключами шифрования** и установите флажок **Разрешить** рядом с разрешением **Запись**, чтобы предоставить пользователю или группе право доступа на **Запись** к функции управления ключами шифрования.

4. После настройки набора прав доступа нажмите на кнопку **OK**.

Набор прав для пользователя или группа пользователей настроен.

Права Сервера администрирования (или группы администрирования) разделены на следующие области:

- Общие функции:
  - Управление группами администрирования
  - Доступ к объектам независимо от их списков ACL
  - Базовая функциональность
  - Удаленные объекты
  - Управление ключами шифрования
  - Обработка событий
  - Операции с Сервером администрирования (только в окне свойств Сервера администрирования)
  - Теги устройств
  - Развертывание приложений "Лаборатории Касперского"
  - Управление лицензионными ключами
  - Интеграция приложения
  - Управление отчетами
  - Иерархия Серверов администрирования
  - Права пользователей
  - Виртуальные Серверы администрирования
- Управление мобильными устройствами:
  - Общие
  - Self Service Portal
- Управление системой:
  - Подключения
  - Удаленное выполнение скриптов
  - Инвентаризация оборудования
  - Network Access Control
  - Развертывание ОС
  - Системное администрирование

- Удаленная установка
- Инвентаризация приложений

Если для права не выбрано ни **Разрешить**, ни **Запретить**, оно считается *неопределенным*: право отклоняется до тех пор, пока оно не будет явно отклонено или разрешено для пользователя.

Права пользователей являются суммой следующего:

- собственных прав пользователя;
- прав всех ролей, назначенных пользователю;
- прав всех групп безопасности, в которые входит пользователь;
- прав всех ролей, назначенных группам, в которые входит пользователь.

Если хотя бы в одном наборе прав есть запрещенное право (для права установлен флажок **Запретить**), тогда для пользователя это право запрещено, даже если в других наборах прав оно разрешено или не определено.

Также вы можете добавить пользователей и группы безопасности в область пользовательской роли, чтобы использовать различные возможности Сервера администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Назначение роли пользователю или группе безопасности

Чтобы назначить роли пользователю или группе безопасности:

1. В главном окне приложения перейдите в раздел U **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.
2. Выберите имя пользователя или группы безопасности, которой нужно назначить роль.

   Можно выбрать несколько имен.
3. В меню нажмите на кнопку **Назначить роль**.

   Будет запущен мастер назначения роли.
4. Следуйте шагам мастера: выберите роль, которую вы хотите назначить выбранным пользователям или группам безопасности, а затем выберите область применения роли.

   Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

В результате роль с набором прав для работы с Сервером администрирования будет назначена пользователю (или пользователям, или группе безопасности). В списке пользователей или групп безопасности отображается флажок в столбце **Имеет назначенные роли**.

Создание роли пользователя

Чтобы создать роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Имя новой роли** укажите имя новой роли.
4. Нажмите на кнопку **OK**, чтобы применить изменения.
5. В открывшемся окне измените параметры роли:
   - На вкладке **Общие** измените имя роли.

     Вы не можете изменять имена предопределенных ролей.
   - На вкладке **Параметры** измените область действия роли, а также политики и профили политик, связанные с ролью.
   - На вкладке **Права доступа** измените права доступа к приложениям "Лаборатории Касперского".
6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Созданная роль появится в списке ролей пользователей.

Изменение роли пользователя

Чтобы изменить роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, которую требуется изменить.
3. В открывшемся окне измените параметры роли:
   - На вкладке **Общие** измените имя роли.

     Вы не можете изменять имена предопределенных ролей.
   - На вкладке **Параметры** измените область действия роли, а также политики и профили политик, связанные с ролью.
   - На вкладке **Права доступа** измените права доступа к приложениям "Лаборатории Касперского".
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Обновленная роль появится в списке ролей пользователей.

Изменение области для роли пользователя

Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Чтобы добавить пользователей, группы пользователей и группы администрирования в область применения роли пользователя, воспользуйтесь одним из следующих способов:

Способ 1:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.

2. Установите флажки напротив имен пользователей или групп пользователей, которые требуется добавить в область роли.

3. Нажмите на кнопку **Назначить роль**.

   Будет запущен мастер назначения роли. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. На шаге **Выбор роли** выберите роль, которую требуется назначить.

5. На шаге **Определение области** выберите группу администрирования, которую требуется добавить в область роли.

6. Нажмите на кнопку **Назначить роль**, чтобы закрыть окно мастера.

Выбранные пользователи или группы пользователей и выбранная группа администрирования добавлены в область применения роли.

Способ 2:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.

2. Выберите роль, для которой требуется задать область.

3. В открывшемся окне свойств роли выберите вкладку **Параметры**.

4. В разделе **Область действия роли** нажмите на кнопку **Добавить**.

   Будет запущен мастер назначения роли. Для продолжения работы мастера нажмите на кнопку **Далее**.

5. На шаге **Определение области** выберите группу администрирования, которую требуется добавить в область роли.

6. На шаге **Выбор пользователей** выберите пользователей и группы пользователей, которые требуется добавить в область применения роли.

7. Нажмите на кнопку **Назначить роль**, чтобы закрыть окно мастера.

8. Закройте окно свойств роли.

Выбранные пользователи или группы пользователей и выбранная группа администрирования добавлены в область применения роли.

Способ 3:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Права доступа** установите флажок рядом с именем пользователя или группы безопасности, которых требуется добавить в область применения пользовательской роли, и нажмите на кнопку **Роли**.

   Вы не можете выбрать несколько пользователей или групп безопасности одновременно. Если вы выберете более одного объекта, кнопка **Роли** будет неактивна.

3. В окне **Роли** выберите пользовательскую роль, которую вы хотите назначить, и нажмите на кнопку **ОК**, чтобы сохранить изменения.

   Выбранные пользователи или группы безопасности добавлены в область роли.

Удаление роли пользователя

Чтобы удалить роль пользователя:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.

2. Установите флажок напротив роли, которую требуется удалить.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **ОК**.

Роль пользователя будет удалена.

Связь профилей политики с ролями

Вы можете связывать роли с профилями политик. В этом случае правило активации для профиля политики определяется в зависимости от роли: профиль политики становится активным для пользователя с определенной ролью.

Например, политика запрещает запуск приложений городской навигации для всех устройств группы администрирования. Приложения городской навигации необходимы для работы только одного устройства пользователя, выполняющего роль курьера, в группе администрирования "Пользователи". В этом случае можно назначить роль "Курьер" владельцу этого устройства и создать профиль политики, разрешающий использовать приложения городской навигации на устройствах, владельцам которых назначена роль "Курьер". Все остальные параметры политики остаются без изменений. Только пользователям с ролью "Курьер" разрешено использовать приложения городской навигации. Затем, если другому сотруднику будет назначена роль "Курьер", этот сотрудник также сможет использовать приложения городской навигации на устройстве, принадлежащем вашей организации. Однако использование приложений городской навигации будет запрещено на других устройствах этой группы администрирования.

Чтобы связать роль с профилем политики:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, которую требуется связать с профилем политики.

   Откроется окно свойств роли на вкладке **Общие**.
3. Перейдите на вкладку **Параметры** и прокрутите вниз до раздела **Политики**.
4. Нажмите на кнопку **Изменить**.
5. Чтобы связать роль с:

   - **Существующим профилем политики** – нажмите на значок (>) рядом с именем требуемой политики, а затем установите флажок рядом с профилем политики, с которым вы хотите связать роль.
   - **Новым профилем политики**:

     a. Установите флажок около политики, для которой вы хотите создать профиль политики.

     b. Нажмите на кнопку **Новый профиль политики**.

     c. Укажите имя нового профиля политики и настройте параметры профиля политики.

     d. Нажмите на кнопку **Сохранить**.

     e. Установите флажок рядом с новым профилем политики.
6. Нажмите на кнопку **Назначить роли**.

Выбранный профиль политики связывается с ролью и появляется в свойствах роли. Профиль автоматически применяется ко всем устройствам, владельцам которых назначена эта роль.

Создание группы безопасности

Чтобы создать группу безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Группы**.
2. Нажмите на кнопку **Новая группа**.

3. В окне **Новая группа** укажите следующие параметры для новой группы безопасности:

   - **Имя**
   - **Описание**

4. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Группа безопасности добавлена в список групп безопасности.

Изменение группы безопасности

Чтобы изменить группу безопасности:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Группы**.
2. Выберите группу безопасности, которую требуется изменить.
3. В открывшемся окне измените параметры группы безопасности:

   - На вкладке **Общие** можно изменить параметры **Имя** и **Описание**. Эти параметры доступны только для внутренних групп безопасности.
   - На вкладке **Пользователи** можно добавить пользователей в группу безопасности. Эти параметры доступны только для внутренних пользователей и внутренних групп безопасности.
   - На вкладке **Роли** можно назначить роль группе безопасности.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Изменения применены к группе безопасности.

Добавление учетных записей пользователей во внутреннюю группу

Учетные записи внутренних пользователей можно добавлять только во внутреннюю группу.

Чтобы добавить учетные записи пользователей в группу:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Установите флажки напротив учетных записей пользователей, которые требуется добавить в группу.
3. Нажмите на кнопку **Назначить группу**.

4. В открывшемся окне **Назначить группу** выберите группу, в которую требуется добавить учетные записи пользователей.

5. Нажмите на кнопку **Назначить**.

Учетные записи пользователей добавлены в группу. Также можно добавить внутренних пользователей в группу, используя параметры группы.

Удаление группы безопасности

Можно удалять только внутренние группы безопасности.

Чтобы удалить группу пользователей:

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Группы**.

2. Установите флажок напротив группы пользователей, которую требуется удалить.

3. Нажмите на кнопку **Удалить** и подтвердите удаление в открывшемся окне.

Группа пользователей удалена.

Настройка ADFS-интеграции

Чтобы разрешить пользователям, зарегистрированным в Active Directory (AD) вашей организации, входить в Kaspersky Security Center Cloud Console, вам необходимо настроить интеграцию со службами Active Directory Federation Services (AD FS).

Kaspersky Security Center Cloud Console поддерживает AD FS 3 (Windows Server 2016) или выше. AD FS должен быть опубликован и доступен в интернете. В качестве сертификата связи служба AD FS использует публичный доверенный сертификат.

Чтобы изменить параметры AD FS-интеграции, вам нужны права доступа для изменения прав пользователей.

Прежде чем продолжить, убедитесь, что вы выполнили опрос Active Directory.

Чтобы настроить AD FS-интеграцию:

1. В главном окне приложения нажмите на имя Сервера администрирования.

Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры интеграции с AD FS**.

3. Скопируйте URL обратного вызова.

   Этот URL понадобится вам для настройки интеграции в Консоли управления AD FS.

4. В Консоли управления AD FS добавьте группу приложений, а затем добавьте приложение, выбрав шаблон **Server application** (названия элементов интерфейса Microsoft приведены на английском языке).

   Консоль управления AD FS генерирует идентификатор клиента для нового приложения. Идентификатор клиента понадобится вам для настройки интеграции в Kaspersky Security Center Cloud Console.

5. В качестве URI перенаправления укажите URL обратного вызова, который вы скопировали в окне свойств Сервера администрирования.

6. Создайте секрет клиента. Секрет клиента понадобится вам для настройки интеграции с Kaspersky Security Center Cloud Console.

7. Сохраните свойства добавленного приложения.

8. Добавьте приложение в созданную группу приложений. Выберите шаблон **Web API**.

9. На вкладке **Identifiers** в список **Relying party identifiers** добавьте идентификатор клиента серверного приложения, которое вы добавили ранее.

10. На вкладке **Client Permissions** в списке **Permitted scopes** выберите **allatclaims** и **openid**.

11. На вкладке **Issuance Transform Rules** добавьте правило, выбрав шаблон **Send LDAP Attributes as Claims**:

    a. Укажите название правила. Например, вы можете назвать его "Group SID".

    b. Выберите **Active Directory** в качестве хранилища атрибутов, а затем сопоставьте **Token-Groups as SIDs** в качестве атрибута LDAP с "Группа SID" в качестве типа исходящего утверждения.

12. На вкладке **Issuance Transform Rules** добавьте правило, выбрав **Send Claims Using a Custom Rule**:

    a. Укажите название правила. Например, ActiveDirectoryUserSID.

    b. В поле **Custom rule** укажите:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
("http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"), query =
";objectSID;{0}", param = c.Value);
```

13. В Kaspersky Security Center Cloud Console снова откройте раздел **Параметры интеграции с AD FS**.

14. Переведите переключатель в положение **Интеграция AD FS Включено**.

15. Перейдите по ссылке **Параметры** и укажите файл содержащий сертификат или несколько сертификатов федерального сервера.

16. Перейдите по ссылке **Параметры интеграции с AD FS** и укажите следующие параметры:

    - **URL издателя**

      URL сервера федерации, работающего в вашей организации.

В частности, Kaspersky Next XDR Expert добавляет '/.well-known/openid-configuration' к URL эмитента и пытается открыть полученный URL (issuer_URL/.well-known/openid-configuration), чтобы узнать конфигурацию эмитента автоматически.

- **Идентификатор клиента**

  Идентификатор клиента, который сервер федерации генерирует для идентификации Kaspersky Security Center Cloud Console. Вы можете найти идентификатор клиента в консоли управления AD FS в окне свойств серверного приложения, соответствующего Kaspersky Security Center Cloud Console.

- **Секрет клиента**

  Вы генерируете секрет клиента в консоли управления AD FS, когда указываете свойства серверного приложения, которое соответствует Kaspersky Security Center Cloud Console.

- **Доменная аутентификация пользователей**

  Участники выбранного вами домена смогут входить в Kaspersky Security Center Cloud Console, используя свои доменные учетные данные. Доменные имена появятся в списке после завершения опроса сети.

- **Имя поля для SID пользователя в идентификаторе токена**

  Имя поля, которое ссылается на идентификатор безопасности (SID) пользователя в токене идентификатора. Название поля необходимо для идентификации пользователя в Kaspersky Security Center Cloud Console. По умолчанию это поле в токене идентификатора называется 'primarysid'.

- **Имя поля для массива SID групп пользователей в идентификаторе токена**

  Имя поля, которое относится к массиву SID групп безопасности Active Directory, в которые входит пользователь. По умолчанию это поле в идентификаторе токена называется 'groupsid'.

17. Сохраните параметры.

Интеграция с AD FS завершена. Чтобы войти в Kaspersky Security Center Cloud Console с учетными данными AD, используйте ссылку в разделе **Параметры интеграции с AD FS** (**Ссылка для входа в Kaspersky с AD FS**).

После входа в Kaspersky Security Center Cloud Console с учетными данными AD распространяются следующие ограничения:

- Раздел **Data Discovery** недоступен в главном меню.
- Элемент **Управление учетной записью** недоступен в верхней панели.
- Вы не можете переключаться между рабочими областями.

При первом входе в Kaspersky Security Center Cloud Console через AD FS, консоль может реагировать с задержкой.

Настройка интеграции с Microsoft Entra ID

Вам необходимо настроить интеграцию с Microsoft Entra ID, чтобы пользователи вашей организации могли входить в Kaspersky Security Center Cloud Console под учетными данными Microsoft Entra ID.

Интеграция с Microsoft Entra ID доступна только для главного Сервера администрирования. Вы не можете настроить интеграцию для подчиненных или виртуальных Серверов администрирования.

Настройка параметров интеграции

Чтобы настроить интеграцию с Microsoft Entra ID:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Microsoft Entra ID**.

3. Включите переключатель **Интеграция с Microsoft Entra ID**.

4. Скопируйте ссылки из следующих полей:

   - **URL обратного вызова**
   - **Веб-адрес выхода из переднего канала**

     Эти адреса понадобятся вам для регистрации Kaspersky Security Center Cloud Console в тенанте Microsoft Entra ID.

   - **Веб-адрес входа**

     Этот URL понадобится вам, чтобы пользователи могли входить в рабочую область Kaspersky Security Center Cloud Console под своими учетными данными Microsoft Entra ID после завершения интеграции с Microsoft Entra ID.

5. Войдите в Microsoft Entra Admin Center и выберите тенант своей организации.

   У вас должна быть роль глобального администратора или администратора приложения в тенанте.

6. В главном меню выберите **Identity** → **Applications** → **App registrations** и нажмите на кнопку **New registration**.

7. В открывшемся окне выполните одно из следующих действий:

   - Укажите имя приложения Kaspersky Security Center Cloud Console.
   - В разделе **Supported account types** выберите параметр **Accounts in this organizational directory only (<tenant_name> only - Single tenant)**.
   - В разделе **Redirect URI** выберите в раскрывающемся списке **Web** и введите URL обратного вызова, который вы скопировали в Kaspersky Security Center Cloud Console на шаге 4.

8. Нажмите на кнопку **Register**.

   Приложение Kaspersky Security Center Cloud Console зарегистрировано в Microsoft Entra ID, и открывается страница обзора приложения.

9. При необходимости добавьте Kaspersky Security Center Cloud Console в список приложений.

   Пользователи смогут открыть приложение Kaspersky Security Center Cloud Console, нажав на его название в списке приложений в Мои приложения и Office 365 Launcher без использования веб-адреса для входа.

10. Скопируйте **Application (client) ID** и **Directory (tenant) ID** и сохраните их любым удобным способом.

    Эти идентификаторы понадобятся вам при заполнении обязательных полей в Kaspersky Security Center Cloud Console на шаге 14.

11. В меню приложения Kaspersky Security Center Cloud Console перейдите в раздел **Authentication** и введите URL, которые вы скопировали из Kaspersky Security Center Cloud Console на шаге 4:

    - В разделе **Web** нажмите на кнопку **Add URI** и введите URL для входа.
    - В разделе **Front-channel logout URL** введите URL выхода из основного канала.

12. В меню приложения Kaspersky Security Center Cloud Console перейдите в раздел **Certificates & secrets** и выполните следующие действия:

    a. Перейдите на вкладку **Client secrets** и нажмите на кнопку **New client secret**.

    b. В открывшемся окне укажите любое описание секрета клиента и выберите период, по истечении которого срок действия секрета истечет.

    > Рекомендуется любым удобным способом скопировать дату, после которой истекает срок действия секрета, чтобы своевременно изменять секреты.

    a. Нажмите на кнопку **Добавить**.

    Созданный секрет отображается на вкладке **Client secrets**.

    b. Скопируйте информацию из столбца **Value**.

    > Рекомендуется скопировать информацию сразу после создания секрета клиента.

13. В меню приложения Kaspersky Security Center Cloud Console перейдите в раздел **Token configuration** и выполните следующие действия:

    - Добавьте необязательное утверждение **onprem_sid**:

        a. Нажмите на кнопку **Add optional claim**.

        b. В открывшемся окне выберите тип токена **ID** и в столбце **Claim** установите флажок рядом с **onprem_sid**.

        c. Нажмите на кнопку **Добавить**.

        Необязательное утверждение **onprem_sid** отображается на странице **Optional claims**.

    - Добавьте необязательное утверждение **preferred_username**:

        a. Нажмите на кнопку **Add optional claim**.

        b. В открывшемся окне выберите тип токена **Access** и в столбце **Claim** установите флажок рядом с **preferred_username**.

        c. Нажмите на кнопку **Добавить**.

        Необязательное утверждение **preferred_username** отображается на странице **Optional claims**.

14. В меню приложения Kaspersky Security Center Cloud Console перейдите в раздел **API permissions** и добавьте разрешения:

    - **User.Read.All**
    - **User.Export.All**
    - **GroupMember.Read.All**
    - **Directory.Read.All**

    Чтобы добавить разрешения:

    a. Нажмите на кнопку **Add a permission** и выберите вкладку **Microsoft API**.

    b. Выберите **Microsoft Graph** → **Application permissions** и выберите разрешение, которое вы хотите добавить.

    c. Нажмите на кнопку **Add permission**.

    Четыре разрешения добавлены и отображаются на странице **Configured permissions**.

    d. Нажмите кнопку **Предоставить согласие администратора для <tenant_name>**, а затем в открывшемся окне нажмите **Да**, чтобы подтвердить предоставление согласия на добавленные вами разрешения.

15. Вернитесь в Kaspersky Security Center Cloud Console и на вкладке **Общие** заполните следующие обязательные поля:

    - **Идентификатор тенанта**. Значение поля **Directory (tenant) ID**, которое вы копируете на шаге 10.
    - **Идентификатор клиента**. Значение поля **Идентификатор приложения (клиента)**, которое вы копируете на шаге 10.
    - **Секрет клиента**. Значение, которое вы копируете на шаге 12.

16. Нажмите на кнопку **Проверить подключение**, чтобы проверить правильность параметров, а затем после отображения статуса **Подключено** нажмите на кнопку **Сохранить**.

Параметры интеграции сохранены, интеграция с Microsoft Entra ID настроена.

Проверка добавления пользователей

После настройки интеграции с Microsoft Entra ID необходимо выполнить следующие действия:

1. В главном окне приложения Kaspersky Security Center Cloud Console перейти в раздел **Пользователи и роли → Пользователи и группы**, чтобы убедиться, что пользователи и группы из Microsoft Entra ID добавлены в Kaspersky Security Center Cloud Console.

   Если пользователи и группы в вашем тенанте Microsoft Entra ID синхронизированы из Active Directory вашей организации и настроен опрос Active Directory, то пользователи и группы уже добавлены в Kaspersky Security Center Cloud Console в результате опроса Active Directory.

   Иначе вам необходимо включить и запустить опрос Microsoft Entra ID, чтобы добавить пользователей и группы из вашего тенанта Microsoft Entra ID в Kaspersky Security Center Cloud Console.

2. Назначить необходимые роли пользователям и группам.

   При назначении ролей пользователю на виртуальном Сервере администрирования в главном окне приложения перейдите в раздел **Пользователи и роли → Пользователи и группы** и выберите вкладку **Пользователи**. Если вы выберете вкладку **Группы** и назначите роли группе, членом которой является пользователь, пользователь не сможет войти в Kaspersky Security Center Cloud Console.

3. Отправить пользователям URL для входа, который вы скопировали на шаге 4. Они будут вводить этот URL для **входа в рабочую область Kaspersky Security Center Cloud Console, используя свои учетные данные Microsoft Entra ID**.

   Когда пользователь выходит из учетной записи Microsoft Entra ID, которую он использовал для аутентификации в Kaspersky Security Center Cloud Console, и приложение Kaspersky Security Center Cloud Console открыто на другой вкладке или в другом окне того же браузера, этот сеанс также заканчивается для Kaspersky Security Center Cloud Console и пользователь автоматически выходит из консоли.

   Если Kaspersky Security Center Cloud Console открыта в другом браузере или на других устройствах, сеанс продолжается, когда пользователь выходит из учетной записи Microsoft Entra ID.

Чтобы войти в Kaspersky Security Center Cloud Console с учетными данными Microsoft Entra ID, пользователи должны иметь возможность войти в свою учетную запись Microsoft Entra ID.

Ограничения

После входа в Kaspersky Security Center Cloud Console с учетными данными Microsoft Entra ID распространяются следующие ограничения:

- Раздел **Data Discovery** недоступен в главном меню.
- Элемент **Управление учетной записью** недоступен в верхней панели.
- Вы не можете переключаться между рабочими областями.

Включение опроса Microsoft Entra ID

Вам нужно включить опрос Microsoft Entra ID, чтобы добавить пользователей из Microsoft Entra ID в Kaspersky Security Center Cloud Console.

В Kaspersky SIEM Cloud вы можете добавить не более 17 000 учетных записей пользователей.

Чтобы включить опрос Microsoft Entra ID:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Microsoft Entra ID**.
3. В разделе **Обнаружение пользователей** включите переключатель **Опрос Microsoft Entra ID**.
4. Если вы хотите изменить расписание опроса по умолчанию, нажмите на кнопку **Параметры расписания**, укажите период и время опроса в открывшемся окне и нажмите на кнопку **Сохранить**.

   Опрос Microsoft Entra ID будет выполняться в соответствии с настроенным расписанием.

5. Если вы хотите запустить опрос Microsoft Entra ID немедленно, нажмите на кнопку **Запустить сейчас**.

   Начнется загрузка пользователей. Когда пользователи загрузятся, опрос Microsoft Entra ID завершится.

6. Нажмите на кнопку **Сохранить**.

Опрос Microsoft Entra ID завершен, пользователи из Microsoft Entra ID добавлены в Kaspersky Security Center Cloud Console.

Добавление Kaspersky Security Center Cloud Console в список приложений

Вы можете разрешить пользователям открывать приложение Kaspersky Security Center Cloud Console, нажав по его названию в списке приложений, не вводя веб-адрес для входа. Список приложений доступен в My Apps и в Office 365 Launcher.

Чтобы добавить Kaspersky Security Center Cloud Console в список приложений:

1. В главном меню центра администрирования Microsoft Entra перейдите в раздел **Identity** → **Applications** → **App registrations**, после чего на вкладке **All applications** выберите приложение Kaspersky Security Center Cloud Console, которое вы ранее зарегистрировали в Microsoft Entra ID.

2. В меню Kaspersky Security Center Cloud Console перейдите в раздел **Branding & properties** и выполните следующие действия:

   a. В поле **Home page URL** введите веб-адрес для входа.

   b. При необходимости в поле **Upload new logo** добавьте изображение, которое будет использоваться в качестве значка приложения в списке приложений.

   c. Нажмите на кнопку **Сохранить**.

3. В главном меню Центра администрирования Microsoft Entra перейдите в раздел **Identity** → **Applications** → **Enterprise applications** и выберите Kaspersky Security Center Cloud Console.

   Откроется страница обзора приложения.

4. В меню Kaspersky Security Center Cloud Console перейдите в раздел **Properties** и выполните следующие действия:

   a. Установите для следующих параметров значение **Да**:

   - **Разрешено ли пользователям входить в систему?**

     Это действие необходимо, только если по умолчанию для параметра не задано значение **Да**.

   - **Видны пользователям?**

   b. Нажмите на кнопку **Сохранить**.

5. В меню Kaspersky Security Center Cloud Console перейдите в раздел **Users and groups** и выполните следующие действия:

   a. Нажмите на кнопку **Add user/group** и перейдите по ссылке **Users and groups**.

   b. В открывшемся окне выберите пользователей и группы и нажмите на кнопку **Save**.

   Окно закрыто.

   c. Нажмите на кнопку **Назначить**.

Приложение Kaspersky Security Center Cloud Console доступно в My Apps и Office 365 Launcher для выбранных пользователей. Пользователи могут открыть приложение Kaspersky Security Center Cloud Console, нажав на его название в списке, без ввода веб-адреса для входа.

Назначение пользователя владельцем устройства

Информацию о назначении пользователя владельцем мобильного устройства см. в справке Kaspersky Security для мобильных устройств.

Чтобы назначить пользователя владельцем устройства:

1. Если вы хотите назначить владельца устройства, подключенного к виртуальному Серверу администрирования, сначала переключитесь на виртуальный Сервер администрирования:

   a. В главном меню нажмите на значок шеврона (›) справа от текущего имени Сервера администрирования.

   b. Выберите требуемый Сервер администрирования.

2. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.

   Откроется список пользователей. Если вы в данный момент подключены к виртуальному Серверу администрирования, в список входят пользователи текущего виртуального Сервера администрирования и главного Сервера администрирования.

3. Нажмите на учетную запись пользователя, которую требуется назначить в качестве владельца устройству.

4. В открывшемся окне свойств пользователя выберите вкладку **Устройства**.

5. Нажмите на кнопку **Добавить**.

6. Из списка устройств выберите устройство, которое вы хотите назначить пользователю.

7. Нажмите на кнопку **ОК**.

Выбранное устройство добавляется в список устройств, назначенных пользователю.

Также можно выполнить эту операцию в группе **Управление активами** → **Управляемые устройства**, выбрав имя устройства, которое вы хотите назначить, и перейдя по ссылке **Сменить владельца устройства**.

Назначение пользователя владельцем устройства Linux после установки Агента администрирования

Чтобы разрешить пользователю зарегистрироваться в качестве владельца устройства Linux:

1. В OSMP Console перейдите в раздел **Управление программным обеспечением** → **Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов.

2. Нажмите на инсталляционный пакет Агента администрирования.

   Отобразится окно свойств инсталляционного пакета.

3. В открывшемся окне свойств инсталляционного пакета перейдите на вкладку **Параметры** → **Дополнительно**.

4. В разделе **Регистрация пользователя в качестве владельца устройства (только для Linux)** включите параметр **Разрешить запуск утилиты регистрации пользователя после установки Агента администрирования** и нажмите на кнопку **Сохранить**.

Утилиту для регистрации пользователя в качестве владельца устройства можно запустить из командной строки на клиентском устройстве.

Чтобы зарегистрировать пользователя в качестве владельца устройства Linux на клиентском устройстве:

1. Выполните следующую команду в командной строке на клиентском устройстве:
   `$ /opt/kaspersky/klnagent64/bin/nagregister -set_owner`

2. Если потребуется, введите учетную запись и пароль.

   Если учетная запись и пароль включены в файл ответов или инсталляционный пакет Агента администрирования, выполните следующую команду в командной строке на клиентском устройстве:
   `$ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended`

Если пользователь входит во внутреннюю группу безопасности, учетная запись должна содержать имя пользователя.

Если пользователь входит в группу безопасности Active Directory, учетная запись должна содержать имя пользователя и имя домена.

Пользователь зарегистрирован как владелец устройства.

Работа с ревизиями объектов

Этот раздел содержит информацию о работе с ревизиями объектов.

Ревизия – это состояние объекта в определенный момент. Каждый раз, когда вы создаете или изменяете объект, создается новая ревизия этого объекта. Каждая ревизия содержит значения всех параметров объекта, актуальных на момент создания или сохранения ревизии.

Объекты, которые поддерживают работу с ревизиями:

- свойства Сервера администрирования;
- политики;
- задачи;
- группы администрирования;
- учетные записи пользователей;
- инсталляционные пакеты.

Вы можете выполнять с ревизиями объектов следующие действия:

- просматривать выбранную ревизию (доступно только для политик);
- откатывать изменения объекта к выбранной ревизии;
- сохранять ревизии в виде файла JSON (доступно только для политик).

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- **Ревизия** – номер ревизии объекта.
- **Время** – дата и время изменения объекта.
- **Пользователь** – имя пользователя, изменившего объект.
- **IP-адрес устройства пользователя** – IP-адрес устройства, с которого был изменен объект.
- **IP-адрес Web Console** – IP-адрес OSMP Console, с помощью которого был изменен объект.
- **Действие** – выполненное действие с объектом.
- **Описание** – описание ревизии изменения параметров объекта.

  По умолчанию описание ревизии объекта не заполнено. Чтобы добавить описание ревизии, выберите нужную ревизию и нажмите на кнопку **Изменить описание**. В открывшемся окне введите текст описания ревизии.

Добавление описания ревизии

Вы можете добавить описание для ревизии, чтобы в дальнейшем было проще найти необходимую ревизию в списке.

Чтобы добавить описание ревизии:

1. В окне свойств объекта перейдите на вкладку **История ревизий**.
2. В списке ревизий объекта выберите ревизию, для которой нужно добавить описание.
3. Нажмите на кнопку **Изменить описание**.

   Откроется окно **Описание**.
4. В окне **Описание** введите текст описания ревизии.

   По умолчанию описание ревизии объекта не заполнено.
5. Сохраните описание ревизии.

Описание добавлено для ревизии объекта.

Откат изменений объекта к предыдущей ревизии

В случае необходимости вы можете откатить изменения объекта. Например, вам может понадобиться вернуть параметры политики к состоянию на определенную дату.

Чтобы откатить изменения объекта:

1. В окне свойств объекта перейдите на вкладку **История ревизий**.
2. В списке ревизий объекта выберите номер ревизии, к которой нужно откатить изменения.
3. Нажмите на кнопку **Откатить**.
4. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

Произойдет откат к выбранной ревизии. В списке ревизий объекта отобразится запись о выполненном действии. В описании ревизии отобразится информация о номере ревизии, к которой вы вернули объект.

Просмотр и сохранение ревизии политики

Ревизия политики — это сохраненное состояние политики, которое автоматически фиксируется каждый раз при ее изменении и сохранении. Ревизия сдержит параметры политики, профили и правила их активации, метаданные о дате, а также пользователе и IP-адресе, которые создали эту ревизию. Open Single Management Platform позволяет просматривать ревизию политики, чтобы отслеживать изменения настроек, а также сохранять ревизию в файл JSON.

Просмотр и сохранение ревизии политики доступны, если соответствующий веб-плагин управления поддерживает эту функцию.
Опции доступны для политик Сервера администрирования, Агента администрирования, Kaspersky Endpoint Security for Windows (начиная с версии веб-плагина 14.0), Kaspersky Endpoint Security for Linux (начиная с версии веб-плагина 12.4) и Kaspersky Endpoint Security for Mac (начиная с версии веб-плагина 12.2.1 Patch A).

Чтобы просмотреть ревизию политики:

1. В главном окне приложения перейдите в раздел **Управление активами → Политики**.
2. Нажмите на ревизию политики, которую вы хотите просмотреть и перейдите в раздел **История ревизий**.
3. В списке ревизий политики нажмите на номер ревизии, которую вы хотите просмотреть.

   В открывшемся отчете доступна информация о параметрах политики, ее профилях и правилах активации для них.

   Если размер ревизии превышает 10 МБ, просмотреть ее с помощью OSMP Console невозможно. Вам будет предложено сохранить выбранную ревизию в файл JSON.

   Если размер ревизии не превышает 10 МБ, отображается отчет в формате HTML с параметрами выбранной ревизии политики. Так как отчет отображается во всплывающем окне, убедитесь, что в вашем браузере разрешены всплывающие окна.

В случае политик Kaspersky Endpoint Security for Windows и Kaspersky Endpoint Security for Mac в отчете не будет информации о профилях политик.

Чтобы сохранить ревизию политики в файл JSON,

В списке ревизий политики выберите ревизию, которую вы хотите сохранить и нажмите на кнопку **Сохранить в файл**.

Ревизия сохранена в файле JSON.

При необходимости вы можете сравнить ревизии политики.

Сравнение ревизий политики

Вы можете сравнить предыдущие ревизии политики с ее текущей ревизией, сравнить различные ревизии, выбранные в списке, или сравнить ревизию одной политики с ревизией другой политики. Параметры доступны для политик Сервера администрирования, Агента администрирования, Kaspersky Endpoint Security for Windows (начиная с версии веб-плагина 14.0) и Kaspersky Endpoint Security for Mac (начиная с версии веб-плагина 12.2.1 Patch A).

Сравнение ревизий политик доступно, если соответствующие веб-плагины управления поддерживает эту функцию.

Чтобы просмотреть ревизию политики:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на политику, ревизии которой вы хотите сравнить.

   Откроется окно свойств политики.
3. Перейдите на вкладку **История ревизий** и установите флажки рядом с ревизиями, которые нужно сравнить.
4. В панели инструментов нажмите на кнопку **Сравнить** и в раскрывающемся списке выберите один из следующих вариантов:

   - **С текущей ревизией**, если вы хотите сравнить ревизию, выбранную на шаге 3, с последней сохраненной ревизией той же политики.
   - **Выбранные ревизии**, если вы хотите сравнить две ревизии, около которых вы установили флажки на шаге 3.

     Порядок установки флажков не влияет на результаты сравнения. По умолчанию более ранняя выбранная ревизия сравнивается с последней ревизией. Например, если вы установите флажки рядом с ревизиями 5 и 1, ревизия 1 будет сравниваться с ревизией 5. Отчет будет содержать информацию о параметрах ревизии 1, которые были добавлены, удалены или изменены по сравнению с ревизией 5.
   - **С ревизией другой политики**, если вы хотите сравнить ревизии двух разных политик.

В открывшейся панели выполните следующие действия:

a. В поле **Название приложения** выберите политику ревизии которой вы хотите сравнить: Агент администрирования или Сервер администрирования.

b. В поле **Название политики** укажите название политики, ревизию которой вы хотите сравнить с той, которую вы выбрали на шаге 3.

Отобразится список ревизий политики.

c. Выберите нужную ревизию и нажмите на кнопку **Сравнить**.

Отчет сравнения ревизий отобразится в формате HTML на новой вкладке вашего браузера.

Если результат сравнения превышает 10 МБ, отобразится соответствующее диалоговое окно. Вы можете нажать на кнопку **Сохранить в файл**, чтобы сохранить отчет в виде файла, или отменить операцию.

Отчет отображается на языке интерфейса вашей OSMP Console. Вы можете развернуть некоторые разделы отчета, нажав на значок стрелки вниз (▼) рядом с разделом или свернуть раздел, нажав на значок стрелки вверх (▲).

Отчет содержит следующую информацию:

- Логотип "Лаборатория Касперского".
- Название отчета.
- Время и дата создания отчета.
- Имя политики, Сервер администрирования и группа администрирования, в которую входит политика (политики), ревизии которой сравнивались.
- Кнопка **Сохранить как HTML**. Если вы нажмете на кнопку, отчет будет сохранен на вашем устройстве.
- Раздел **Сводная информация**, в котором отображается общая информация о сравниваемых ревизиях: имя политики (политик), номер ревизии, время и дата, когда ревизия была сохранена, пользователь, который сохранил ревизию, и описание ревизии.

  Для унаследованных политик пользователь не отображается.

- Различия сравниваемых ревизий. Различия отображаются в следующих разделах:
  - **Добавленные параметры.**
  - **Удаленные параметры.**
  - **Измененные параметры.**
  - **Параметры доступны только для объекта 1** (если вы сравнивали ревизии двух разных политик).
  - **Параметры доступны только для объекта 2** (если вы сравнивали ревизии двух разных политик).

Раздел не отображается, если в нем нет данных.

Kaspersky Security Network (KSN)

В этом разделе описано использование инфраструктуры онлайн-служб Kaspersky Security Network (KSN). Приведена информация о KSN, а также инструкции по включению KSN, настройке доступа к KSN, по просмотру статистики использования прокси-сервера KSN.

Функциональность KSN может быть недоступна в решении на территории США.

О KSN

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. KSN позволяет получать из репутационных баз "Лаборатории Касперского" информацию о приложениях, установленных на клиентских устройствах.

Участвуя в программе KSN, вы соглашаетесь в автоматическом режиме предоставлять в "Лабораторию Касперского" информацию о работе приложений "Лаборатории Касперского", установленных на клиентских устройствах, находящихся под управлением Open Single Management Platform. Передача информации выполняется в соответствии с настроенными параметрами доступа к KSN. Специалисты "Лаборатории Касперского" дополнительно анализируют полученную информацию и включают ее в репутационные и статистические базы данных Kaspersky Security Network.

Приложение предлагает присоединиться к KSN во время работы мастера первоначальной настройки. Вы можете начать использование KSN или отказаться от использования KSN в любой момент работы с приложением.

Вы используете KSN в соответствии с Положением о KSN, которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования или при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с предыдущей версией Положения о KSN, которую вы приняли ранее.

Когда KSN включен, Open Single Management Platform проверяет доступность серверов KSN. Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы. Это необходимо, чтобы убедиться, что уровень безопасности поддерживается для управляемых устройств.

Клиентские устройства, находящиеся под управлением Сервера администрирования, взаимодействуют с KSN при помощи службы прокси-сервера KSN. Служба прокси-сервера KSN предоставляет следующие возможности:

- Клиентские устройства могут выполнять запросы к KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет.
- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

Можно включить прокси-сервер KSN на стороне точки распространения, чтобы устройство исполняло роль прокси-сервера KSN. В этом случае на устройстве запустится служба прокси-сервера KSN (ksnproxy).

Включение и отключение KSN

Чтобы включить KSN:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры KSN**.

3. Переведите переключатель **Kaspersky Security Network** в положение **Включено**.

   KSN включен.

   Если переключатель включен, клиентские устройства будут передавать результаты установки патчей в "Лабораторию Касперского". Включая переключатель, вам нужно прочитать и принять условия Положения о KSN.

4. Нажмите на кнопку **Сохранить**.

Чтобы выключить KSN:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры KSN**.

3. Переведите переключатель **Kaspersky Security Network** в положение **Выключено**.

   KSN выключен.

   Если переключатель выключен, клиентские устройства не будут передавать результаты установки патчей в "Лабораторию Касперского".

4. Нажмите на кнопку **Сохранить**.

Просмотр принятого Положения о KSN

При включении Kaspersky Security Network (KSN) вам нужно прочитать и принять Положение о KSN. Вы можете просмотреть принятое Положение о KSN в любое время.

Чтобы просмотреть принятое Положение о KSN:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Параметры KSN**.

3. Перейдите по ссылке **Просмотреть Положение о Kaspersky Security Network**.

В открывшемся окне вы можете просмотреть текст принятого Положения о KSN.

Принятие обновленного Положения о KSN

Вы используете KSN в соответствии с Положением о KSN, которое вы читаете и принимаете при включении KSN. Если Положение о KSN было обновлено, оно автоматически отображается при открытии Kaspersky Security Center Cloud Console. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с версией Положения о KSN, которую вы приняли ранее. Вы можете просмотреть и принять обновленное Положение о KSN позже.

Чтобы просмотреть и принять или отклонить обновленное Положение о KSN:

1. Нажмите на значок **Просмотреть уведомления о событиях** в правом верхнем углу главного окна приложения.

   Откроется окно **Уведомления**.

2. Перейдите по ссылке **Просмотреть обновленное Положение о KSN**.

   Откроется окно **Обновление Положения о Kaspersky Security Network**.

3. Прочтите Положение о KSN, а затем примите решение, нажав одну из следующих кнопок:

   - **Я принимаю условия обновленного Положения о KSN**
   - **Использовать KSN со старым Положением о KSN**

В зависимости от вашего выбора KSN продолжит работу в соответствии с условиями текущего или обновленного Положения о KSN. Вы можете в любой момент просмотреть текст принятого Положения о KSN в свойствах Сервера администрирования.

Проверка, работает ли точка распространения как прокси-сервер KSN

На управляемом устройстве, которое выполняет роль точки распространения, вы можете включить прокси-сервер KSN. Управляемое устройство работает как прокси-сервер KSN, если на нем запущена служба ksnproxy. Вы можете проверить включить или выключить эту службу на устройстве локально.

Вы можете назначить устройство с операционной системой Windows или Linux в качестве точки распространения. Способ проверки точки распространения зависит от операционной системы этой точки распространения.

Чтобы проверить, работает ли точка распространения с операционной системой Windows как прокси-сервер KSN:

1. На устройстве, которое выполняет роль точки распространения, в Windows откройте окно **Службы** (**Все приложения** → **Администрирование** → **Службы**).

2. В списке служб проверьте, запущена ли служба прокси-сервера KSN – ksnproxy.

   Если служба ksnproxy запущена, то Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN Proxy для управляемых устройств, входящих в область действия точки распространения.

При необходимости службу ksnproxy можно выключить. В этом случае Агент администрирования на точке распространения больше не участвует в Kaspersky Security Network. Для этого требуются права локального администратора.

Чтобы проверить, работает ли точка распространения с операционной системой Linux как прокси-сервер KSN:

1. На устройстве, выполняющем роль точки распространения, отобразится список запущенных процессов.

2. В списке запущенных процессов проверьте запущен ли процесс `/opt/kaspersky/ksc64/sbin/ksnproxy`.

Если процесс `/opt/kaspersky/ksc64/sbin/ksnproxy` запущен, то Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN для управляемых устройств, входящих в область действия точки распространения.

Удаление объектов

Вы можете удалять следующие объекты:

- политики;
- задачи;
- инсталляционные пакеты;
- виртуальные Серверы администрирования;
- пользователей;
- группы безопасности;
- группы администрирования.

Когда вы удаляете объект, информация об этом записывается в базу данных. Срок хранения информации об удаленных объектах такой же, как и срок хранения ревизий объектов (рекомендуемый срок 90 дней). Можно изменить время хранения только при наличии права на **Изменение** для области **Удаленные объекты**.

Об удалении клиентских устройств

При удалении управляемого устройства из группы администрирования программа перемещает устройство в группу Нераспределенные устройства. После удаления устройства установленные приложения "Лаборатории Касперского" – Агент администрирования и приложение безопасности, например Kaspersky Endpoint Security, – остаются на устройстве.

Kaspersky Next XDR Expert обрабатывает устройства из группы Нераспределенные устройства по следующим правилам:

- Если вы настроили правила перемещения устройств и устройство соответствует критериям правила перемещения, устройство автоматически перемещается в группу администрирования в соответствии с правилом.

- Устройство сохраняется в группе Нераспределенные устройства и автоматически удаляется из группы в соответствии с правилами хранения устройств.

  Правила хранения устройств не влияют на устройства, на которых один или несколько дисков зашифрованы с помощью шифрования диска BitLocker. Такие устройства не удаляются автоматически – вы можете удалить их только вручную. Если вам нужно удалить устройство с зашифрованным жестким диском, сначала расшифруйте диск, а затем удалите устройство.

  > При удалении устройства с зашифрованным жестким диском данные, необходимые для расшифровки диска, также удаляются. Если вы установите флажок **Я понимаю риск и хочу удалить устройство (или устройства)** в окне подтверждения, которое открывается при удалении таких устройств (из группы **Нераспределенные устройства** или из группы **Управляемые устройства**), это означает, что вы знаете о последующем удалении данных.

  Чтобы расшифровать диск требуется выполнение следующих условий:

  - Устройство повторно подключается к Серверу администрирования для восстановления данных, необходимых для расшифровки диска.

  - Пользователь устройства помнит пароль для расшифровки.

  - Приложение безопасности, которое использовалось для шифрования диска, например Kaspersky Endpoint Security for Windows, установлено на устройстве.

> В VDI, если у вас есть устройство с зашифрованными жесткими дисками, информация на зашифрованном диске удаляется после удаления устройства.

При удалении устройства из группы Нераспределенные устройства вручную приложение удаляет устройство из списка. После удаления устройства установленные приложения "Лаборатории Касперского" (если они есть) остаются на устройстве. Затем, если устройство по-прежнему видно Серверу администрирования и вы настроили регулярный опрос сети, Kaspersky Next XDR Expert обнаружит устройство во время опроса сети и снова добавит его в группу Нераспределенные устройства. Поэтому удалять устройство вручную целесообразно только в том случае, если оно невидимо для Сервера администрирования.

Обновление баз и приложений "Лаборатории Касперского"

В этом разделе описаны шаги, которые вам нужно выполнить для регулярных обновлений:

- баз и модулей приложений "Лаборатории Касперского";
- установленных приложений "Лаборатории Касперского", включая компоненты Open Single Management Platform и приложений безопасности.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"

В этом разделе представлен сценарий регулярного обновления баз данных, модулей приложений и приложений "Лаборатории Касперского". После того, как вы завершили сценарий Настройка защиты в сети организации вам нужно поддерживать надежность системы защиты. Это обслуживание обеспечит постоянную защиту управляемых устройств от различных угроз, включая вирусы, сетевые атаки и фишинговые атаки.

Существует несколько схем, которые вы можете использовать для установки обновлений компонентов Open Single Management Platform и приложений безопасности. Выберите одну или несколько схем, которые лучше всего соответствуют требованиям вашей сети.

Сценарий ниже описывает схему обновления, которая подразумевает загрузку обновлений в хранилища точек распространения. Если у управляемых устройств нет соединения с точками распространения, рассмотрите возможность обновления баз, модулей приложений и приложений "Лаборатории Касперского" вручную или напрямую с серверов обновлений "Лаборатории Касперского".

После завершения этого сценария вы получите следующие результаты:

- Компоненты Open Single Management Platform обновлены автоматически либо только тогда, когда вы устанавливаете обновлениям статус *Одобрено*.
- Приложения безопасности, базы и модули приложений "Лаборатории Касперского" обновлены в соответствии с расписанием. По умолчанию приложения безопасности "Лаборатории Касперского" устанавливают только те обновления, которые вы одобрили.

Вы можете настроить процесс обновления для загрузки и установки обновлений любым из двух способов:

- Автоматически

  В этом случае вам нужно выполнить этот только сценарий один раз. Вам нужно будет настроить расписание задачи *Загрузка обновлений в хранилища точек распространения* (если есть), задачи Обновление для приложений безопасности "Лаборатории Касперского" и сохранить параметры обновления по умолчанию в свойствах Агента администрирования.

- Вручную

  Вы можете настроить процесс обновления так, чтобы вручную запускать задачу *Загрузка обновлений в хранилища точек распространения* и задачу Обновление для приложений безопасности "Лаборатории Касперского". Вы также можете настроить Агент администрирования на установку обновлений для компонентов Open Single Management Platform только в том случае, если вы устанавливаете статус обновлениям *Одобрено*.

Предварительные требования

Прежде чем приступать, убедитесь, что вы выполнили следующее:

1. Развернуты приложения безопасности "Лаборатории Касперского" на управляемых устройствах в соответствии со сценарием развертывания приложений "Лаборатории Касперского" с помощью OSMP Console. После выполнения этого сценария назначено нужное количество точек распространения в соответствии с количеством управляемых устройств и топологией сети.

2. Созданы и настроены все необходимые политики, профили политик и задачи в соответствии со сценарием настройки защиты сети.

Этапы

Настройка регулярного обновления баз и приложений "Лаборатории Касперского" состоит из следующих этапов:

1. **Создание задачи загрузки обновлений в хранилища точек распространения**

   Создание задачи *Загрузка обновлений в хранилища точек распространения*. После запуска этой задачи Open Single Management Platform загружает обновления на точки распространения непосредственно с серверов обновлений "Лаборатории Касперского".

   Инструкция: Создание задачи загрузки обновлений в хранилища точек распространения

2. **Настройка точек распространения**

   Убедитесь, что параметр **Включено** включен в свойствах всех требуемых точек распространения. Если этот параметр выключен для точки распространения, устройства, включенные в область действия точки распространения, могут загружать обновления только из локального ресурса или напрямую с серверов обновлений "Лаборатории Касперского".

   Если вы хотите, чтобы управляемые устройства получали обновления только от точек распространения, включите параметр **Распространять файлы только через точки распространения** в политике Агента администрирования.

3. **Оптимизация процесса с использованием загрузки файлов различий (если требуется)**

   Включение этой функции приводит к уменьшению трафика между точками распространения и управляемыми устройствами. Чтобы использовать эту функцию, включите параметр **Скачать файлы различий** в свойствах задачи *Загрузка обновлений в хранилища точек распространения*.

   Инструкция: Использование файлов различий для обновления баз и модулей приложений "Лаборатории Касперского"

4. **Определение обновлений для установки**

По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Измените статус на *Одобрено* или *Отклонено*, чтобы определить, следует ли устанавливать это обновление на сетевые устройства. Одобренные обновления всегда устанавливаются. Неопределенные обновления могут быть установлены только на Агенте администрирования и других компонентах Kaspersky SIEM Cloud в соответствии с параметрами политики Агента администрирования. Обновления, которым вы установили статус *Отклонено*, не устанавливаются на управляемые устройства.

Инструкции:

- О статусах обновлений
- Одобрение и отклонение обновлений программного обеспечения

5. **Настройка автоматической установки обновлений и патчей для компонентов Kaspersky SIEM Cloud**

   По умолчанию загруженные обновления и патчи для Агента администрирования и других компонентов Kaspersky SIEM Cloud устанавливаются автоматически. Если вы оставили включенным параметр **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"** в свойствах Агента администрирования, тогда все обновления будут установлены автоматически после их загрузки в хранилище (или несколько хранилищ). Если флажок снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.

   Инструкция: Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky SIEM Cloud

6. **Настройка автоматической установки обновлений для приложений безопасности**

   Создайте задачу "Обновление" для управляемых приложений, чтобы обеспечить своевременное обновление приложений, модулей приложений и баз данных "Лаборатории Касперского", в том числе антивирусных баз. Рекомендуется при настройке расписания задачи выбрать вариант **При загрузке обновлений в хранилище**. Это обеспечит установку новых обновлений как можно раньше.

   По умолчанию обновления для управляемых приложений устанавливаются только после изменения статуса обновления на *Одобрено*. Для Kaspersky Endpoint Security для Windows вы можете изменить параметры обновления в задаче Обновление.

   Если обновление требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства.

   Инструкция: Автоматическая установка обновлений Kaspersky Endpoint Security на устройства

7. **Одобрение и отклонение обновлений управляемых приложений "Лаборатории Касперского"**

   По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус обновления на *Одобрено* или *Отклонено*. Одобренные обновления всегда устанавливаются. Если обновление управляемых приложений "Лаборатории Касперского" требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства. Обновления, которым вы установили статус *Отклонено*, не устанавливаются на управляемые устройства. Если ранее отклоненное обновление для управляемого приложения было установлено, Open Single Management Platform попытается удалить обновления со всех устройств.

   Одобрение и отклонение обновлений доступно только для Агента администрирования и управляемых приложений "Лаборатории Касперского", установленных на клиентских устройствах под управлением Windows и Linux. Бесшовное обновление Сервера администрирования, OSMP Console и веб-плагинов управления не поддерживается.

   Инструкция: Одобрение и отклонение обновлений программного обеспечения.

По завершении сценария можно перейти к мониторингу состояния сети.

Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского"

Чтобы убедиться, что защита ваших управляемых устройств актуальна, вам нужно своевременно обеспечивать обновления следующего:

- Баз и модулей приложений "Лаборатории Касперского".

  Open Single Management Platform проверяет доступность серверов "Лаборатории Касперского" перед загрузкой баз и модулей приложений "Лаборатории Касперского". Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы. Это необходимо для обновления антивирусных баз и поддержания уровня безопасности управляемых устройств.

- установленных приложений "Лаборатории Касперского", включая компоненты Open Single Management Platform и приложений безопасности.

Эксперты "Лаборатории Касперского" обрабатывают все необходимые обновления для Open Single Management Platform и его компонентов, а также для управляемых приложений "Лаборатории Касперского". Вы не можете выполнить эти обновления вручную.

В зависимости от конфигурации вашей сети можно использовать следующие схемы загрузки и распространения необходимых обновлений на управляемые устройства:

- Использование задачи *Загрузка обновлений в хранилища точек распространения*.
- Вручную через локальную папку, общую папку или FTP-сервер.
- Непосредственно с серверов обновлений "Лаборатории Касперского" для приложений безопасности на управляемых устройствах.

Использование задачи Загрузка обновлений в хранилища точек распространения

В этой схеме Open Single Management Platform загружает обновления с помощью задачи *Загрузка обновлений в хранилища точек распространения*. Управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения (см. рисунок ниже).

Точки распространения под управлением macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского".

Если устройства с операционной системой macOS находятся в области действия задачи *Загрузка обновлений в хранилища точек распространения*, задача завершится со статусом *Сбой*, даже если она успешно завершилась на всех устройствах с операционной системой Windows.

Обновление с использованием задачи Загрузка обновлений в хранилища точек распространения

После завершения задачи *Загрузка обновлений в хранилища точек распространения* следующие обновления загружаются в хранилище точка распространения:

- Базы и модули приложений "Лаборатории Касперского" для приложений безопасности на управляемых устройствах.

  Эти обновления устанавливаются с помощью задачи Обновление Kaspersky Endpoint Security для Windows.

- Обновления для компонентов Open Single Management Platform.

  По умолчанию эти обновления устанавливаются автоматически. Вы можете изменить параметры политики Агента администрирования.

- Обновления для приложений безопасности.

  По умолчанию приложение Kaspersky Endpoint Security для Windows устанавливает только те обновления, которые вы одобрили. Обновления устанавливаются с помощью задачи Обновление и могут быть настроены в свойствах этой задачи.

Каждое управляемое приложение "Лаборатории Касперского" запрашивает требуемые обновления с Сервера администрирования. Сервер администрирования объединяет эти запросы и загружает в хранилища точек распространения только те обновления, которые запрашиваются приложениями. Это обеспечивает то, что загружаются только нужные обновления и только один раз. При выполнении задачи *Загрузка обновлений в хранилища точек распространения*, для обеспечения загрузки необходимых версий баз и модулей приложений "Лаборатории Касперского", на серверы обновлений "Лаборатории Касперского" автоматически, Сервер администрирования отправляет следующую информацию:

- идентификатор и версия приложения;
- идентификатор установки приложения;
- идентификатор активного ключа;
- идентификатор запуска задачи Загрузка обновлений в хранилище.

Передаваемая информация не содержит персональных данных и других конфиденциальных данных. АО "Лаборатория Касперского" защищает полученную информацию в соответствии с установленными законом требованиями.

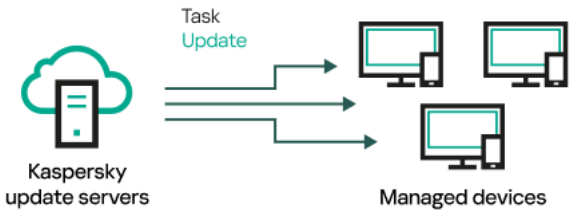
С помощью локальной папки, общей папки или FTP-сервера

Если клиентские устройства не подключены к точке распространения, можно использовать локальную папку или общий ресурс в качестве источника обновления баз, модулей приложений и приложений "Лаборатории Касперского". В этой схеме вам нужно скопировать необходимые обновления из хранилищ точек распространения на съемный диск, а затем обновления копируются в локальную папку или общий ресурс, указанный в качестве источника обновлений в параметрах Kaspersky Endpoint Security для Windows (см. рисунок ниже).

Обновление через локальную папку, общую папку или FTP-сервер

Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security для Windows на управляемых устройствах

На управляемых устройствах Kaspersky Endpoint Security для Windows получает обновления напрямую с серверов обновлений "Лаборатории Касперского" (см. рисунок ниже).



Обновление приложений безопасности непосредственно с серверов обновлений "Лаборатории Касперского"

В этой схеме приложения безопасности не используют хранилища, предоставленные Open Single Management Platform. Чтобы получать обновления непосредственно с серверов обновлений "Лаборатории Касперского", укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений в интерфейсе приложения безопасности. Полное описание этих параметров приведено в документации Kaspersky Endpoint Security для Windows.

Создание задачи загрузки обновлений в хранилища точек распространения

Точки распространения под управлением macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского".

Если устройства с операционной системой macOS находятся в области действия задачи *Загрузка обновлений в хранилища точек распространения*, задача завершится со статусом *Сбой*, даже если она успешно завершилась на всех устройствах с операционной системой Windows.

Вы можете создать задачу *Загрузка обновлений в хранилища точек распространения* для группы администрирования. Такая задача будет выполняться для точек распространения, входящих в указанную группу администрирования.

Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилища точек распространения. Список обновлений включает:

- обновления баз и модулей приложений для приложений безопасности "Лаборатории Касперского";
- обновления компонентов Kaspersky SIEM Cloud;
- обновления приложений безопасности "Лаборатории Касперского".

После загрузки обновлений их можно распространять на управляемые устройства.

Чтобы создать задачу Загрузка обновлений в хранилища точек распространения для выбранной группы администрирования:

1. в главном окне приложения перейдите в раздел **Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. Для приложения Kaspersky SIEM Cloud выберите в поле **Тип задачи** выберите **Загрузка обновлений в хранилища точек распространения**.

4. Укажите название задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

5. Нажмите на кнопку выбора, чтобы указать группу администрирования, выборку устройств или устройства, к которым применяется задача.

6. Если вы включите параметр **Завершение создания задачи** на шаге **Открыть окно свойств задачи после ее создания**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

7. Нажмите на кнопку **Создать**.

   Задача будет создана и отобразится в списке задач.

8. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

9. На вкладке **Параметры приложения** окна свойств задачи укажите следующие параметры:

   - **Источники обновлений**

     В качестве источника обновлений для точки распространения могут быть использованы следующие ресурсы:

     - Серверы обновлений "Лаборатории Касперского"

       HTTP-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложения.

       По умолчанию этот вариант выбран.

     - Локальная или сетевая папка

       Локальная или сетевая папка, которая содержит последние обновления. В качестве сетевой папки можно использовать только смонтированную общую папку SMB. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

       В задачах *Загружать обновления в хранилище Сервера администрирования* и *Загружать обновления в хранилища точек распространения* аутентификация пользователя не работает, если в качестве источника обновлений выбрана защищенная паролем локальная или сетевая папка. Чтобы решить эту проблему, сначала смонтируйте защищенную паролем папку, а затем укажите необходимые учетные данные, например, средствами операционной системы. После этого вы можете выбрать эту папку в качестве источника обновлений в задаче загрузки обновлений. Open Single Management Platform не потребует от вас ввода учетных данных.

- **Папка для хранения обновлений**

  Путь к указанной папке для хранения сохраненных обновлений. Вы можете скопировать указанный путь к папке в буфер обмена. Вы не можете изменить путь к указанной папке для групповой задачи.

- **Скачать файлы различий**

  Этот параметр включает функцию загрузки файлов различий.

  По умолчанию параметр выключен.

- **Скачивать обновления, используя старую схему**

  Начиная с версии 14, Kaspersky Security Center загружает обновления баз и модулей приложений по новой схеме. Чтобы приложение могло загружать обновления с помощью новой схемы, источник обновлений должен содержать файлы обновлений с метаданными, совместимыми с новой схемой. Если источник обновлений содержит файлы обновлений с метаданными, совместимыми только со старой схемой, включите параметр **Скачивать обновления, используя старую схему**. Иначе задача загрузки обновлений завершится ошибкой.

  Например, этот параметр необходимо включить, если в качестве источника обновлений указана локальная или сетевая папка и файлы обновлений в этой папке были загружены одной из следующих приложений:

  - Kaspersky Update Utility

    Эта утилита загружает обновления по старой схеме.

  - Kaspersky Security Center 13 Linux

    Например, точка распространения настроена на получение обновлений из локальной или сетевой папки. В этом случае вы можете загружать обновления с помощью Сервера администрирования, подключенного к интернету, а затем помещать обновления в локальную папку на точке распространения. Если Сервер администрирования имеет номер версии 13, включите параметр **Скачивать обновления, используя старую схему** в задаче *Загружать обновления в хранилища точек распространения*.

  По умолчанию параметр выключен.

10. Создайте расписания запуска задачи. При необходимости настройте следующие параметры:

- **Запуск задачи**

  Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

  - **Вручную** (выбрано по умолчанию)

    Задача не запускается автоматически. Вы можете запустить задачу только вручную.

    По умолчанию выбран этот вариант.

  - **Каждые N минут**

    Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

    По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

  - **Каждый N час**

    Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

По умолчанию задача запускается каждые 6 часов, начиная с текущих системной даты и времени.

- **Каждые N дней**

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются приложением, для которого вы создаете задачу.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

  По умолчанию задача запускается каждую пятницу в текущее системное время.

- **Ежедневно (не поддерживается переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky SIEM Cloud.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Ежемесячно в выбранный день**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию указано время 18:00 и не выбраны дни месяца.

  > Обратите внимание, что вы выбираете порядковый номер дня недели в месяце, а не конкретную дату в месяце или номер недели (первая, вторая неделя месяца). Например, если вы выберите ячейку **Вт** в строке **Первая**, в этом случае задача будет запускаться каждый первый вторник каждого нового месяца.

  Вы можете выбрать несколько дней недели.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы приложений, которые будут отслеживать вирусные атаки. Доступны следующие типы приложений:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы приложений.

  Вы можете запускать разные задачи в зависимости от типа приложения безопасности, сообщающего о вирусной атаке. В этом случае удалите выбор типов приложений, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам. Например, вы можете запустить задачу *Управление устройствами* с помощью параметра **Включить устройство** и после ее завершения запустить задачу *Поиск вирусов*, как запускающую задачу.

  Вам нужно выбрать запускающую задачу из таблицы и статус, с которым эта задача должна завершиться (**Завершена успешно** или **Сбой**).

  При необходимости вы можете искать, сортировать и фильтровать задачи в таблице следующим образом:

  - Введите название задачи в поле поиска, чтобы выполнить поиск задачи по названию.
  - Нажмите на значок сортировки, чтобы отсортировать задачи по имени.

    По умолчанию задачи отсортированы в алфавитном порядке по возрастанию.
  - Нажмите на значок фильтра и в открывшемся окне отфильтруйте задачи по группам, после чего нажмите на кнопку **Применить**.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию. Для расписания **Вручную**, **Один раз** и **Немедленно** задачи выполняются только на тех клиентских устройствах, которые видны в сети. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию параметр включен.

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

11. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

В результате выполнения задачи *Загрузка обновлений в хранилища точек распространения* обновления баз и модулей приложений копируются с источника обновлений и размещаются в папке общего доступа. Загруженные обновления будут использоваться только теми точками распространения, которые входят в указанную группу администрирования и для которых нет явно заданной задачи получения обновлений.

Настройка управляемых устройств для получения обновлений только от точек распространения

Управляемые устройства могут получать обновления баз, модулей приложений и приложения "Лаборатории Касперского" из различных источников: непосредственно с серверов обновлений, от точек распространения, из локальной или сетевой папки. Вы можете указать точки распространения в качестве единственно возможного источника обновлений.

Чтобы настроить получение обновлений управляемыми устройствами только от точек распространения:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на политику Агента администрирования.
3. В окне свойств политики откройте вкладку **Параметры приложения**.
4. В разделе **Параметры** включите переключатель **Распространять файлы только через точки распространения**.

5. Установите замок (🔒) для этого переключателя.

6. Нажмите на кнопку **Сохранить**.

Политика будет применена к выбранным устройствам и устройства будут получать обновления только от точек распространения.

Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky SIEM Cloud

Автоматическая установка обновлений для компонентов Kaspersky SIEM Cloud включена по умолчанию при установке Агента администрирования на устройство. Вы можете выключить ее при установке Агента администрирования или же выключить позже с помощью политики.

Чтобы выключить автоматическую установку обновлений и патчей для компонентов Kaspersky SIEM Cloud при локальной установке Агента администрирования на устройство:

1. Запустите локальную установку Агента администрирования на устройство.

2. На шаге **Дополнительные параметры** снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**.

3. Следуйте далее указаниям мастера.

На устройстве будет установлен Агент администрирования с выключенной автоматической установкой обновлений и патчей для компонентов Kaspersky SIEM Cloud. Вы можете включить автоматическую установку позже с помощью политики.

Чтобы выключить автоматическую установку обновлений для компонентов Kaspersky SIEM Cloud при установке Агента администрирования на устройство с помощью инсталляционного пакета:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Инсталляционные пакеты**.

2. Нажмите на пакет **Агент администрирования Kaspersky Security Center <номер версии>**.

3. В окне свойств выберите вкладку **Параметры**.

4. Выключите переключатель **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**.

Агент администрирования будет устанавливаться из этого пакета с выключенной автоматической установкой обновлений и патчей для компонентов Kaspersky SIEM Cloud. Вы можете включить автоматическую установку позже с помощью политики.

Если при установке Агента администрирования на устройство флажок был установлен (снят) на шаге 4, впоследствии вы можете выключить (включить) автоматическую установку с помощью политики Агента администрирования.

Чтобы включить или выключить автоматическую установку обновлений и патчей для компонентов Kaspersky SIEM Cloud с помощью политики Агента администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на политику Агента администрирования.
3. В окне свойств политики выберите раздел **Параметры приложения**.
4. В разделе **Управление патчами и обновлениями** установите включите или выключите переключатель **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"** чтобы включить или выключить автоматическую установку обновлений и патчей.
5. Убедитесь, что установлен (**Принудительно**) замок (🔒) для этого переключателя.

Политика применится к выбранным устройствам, и автоматическая установка обновлений и патчей для компонентов Kaspersky SIEM Cloud будет включена (выключена) на этих устройствах.

Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows

Вы можете настроить автоматическое обновление баз и модулей приложения Kaspersky Endpoint Security для Windows на клиентских устройствах.

Чтобы настроить загрузку и автоматическую установку обновлений Kaspersky Endpoint Security для Windows на устройства:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Endpoint Security для Windows выберите подтип задачи **Обновление**.
4. Укажите название задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите область действия задачи.
6. Укажите группу администрирования, выборку устройств или устройства, к которым применяется задача.
7. Если вы включите параметр **Завершение создания задачи** на шаге **Открыть окно свойств задачи после ее создания**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
8. Нажмите на кнопку **Создать**.

   Задача будет создана и отобразится в списке задач.
9. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

10. В окне свойств задачи обновления на вкладке **Параметры приложения** укажите локальный или мобильный режим:

    - **Локальный режим**. Параметры на этой вкладке определяют, как устройство получает обновления, когда устанавливается соединение между устройством и Сервером администрирования.

    - **Мобильный режим**. Параметры на этой вкладке определяют, как устройство получает обновления, когда не установлено соединение между Kaspersky SIEM Cloud и устройством (например, если устройство не подключено к интернету).

11. Включите источники обновлений, которые вы хотите использовать для обновления баз и модулей приложения для Kaspersky Endpoint Security для Windows. Если требуется изменить положение источников обновлений в списке, используйте кнопки **Вверх** и **Вниз**. Если включено несколько источников обновлений, Kaspersky Endpoint Security для Windows пытается подключиться к ним один за другим, начиная с верхней части списка, и выполняет задачу обновления, извлекая пакет обновления из первого доступного источника.

    Если в качестве источника обновлений установлено приложение Open Single Management Platform, обновления загружаются из хранилища точки распространения, а не из хранилища Сервера администрирования. Убедитесь, что вы назначили точки распространения и создали задачу *Загрузка обновлений в хранилища точек распространения*.

12. Включите параметр **Устанавливать одобренные обновления модулей приложений**, чтобы загружать и устанавливать обновления модулей приложений вместе с базами приложений.

    Если параметр включен, то Kaspersky Endpoint Security для Windows уведомляет пользователя о доступных обновлениях модулей приложения и во время выполнения задачи обновления включает обновления модулей приложения в пакет обновлений. Kaspersky Endpoint Security для Windows устанавливает только те обновления, для которых вы установили статус *Одобрено*; обновления будут установлены локально через интерфейс приложения или через Kaspersky SIEM Cloud.

    Вы также можете включить параметр **Автоматически устанавливать критические обновления модуля приложения**. При наличии обновлений модулей приложения Kaspersky Endpoint Security для Windows устанавливает обновления со статусом *Предельный* автоматически; остальные обновления модулей приложения – после одобрения их установки администратором.

    Если обновление модулей приложения предполагает ознакомление и согласие с положениями Лицензионного соглашения и Политики конфиденциальности, то приложение устанавливает обновление после согласия пользователя с положениями Лицензионного соглашения и Политики конфиденциальности.

13. Установите флажок **Копировать обновления в папку**, чтобы приложение сохраняло загруженные обновления в папку, а затем укажите путь к папке.

14. Задайте расписание запуска задачи. Чтобы обеспечить своевременное обновление, рекомендуется выбрать вариант **При загрузке обновлений в хранилище**.

15. Нажмите на кнопку **Сохранить**.

При выполнении задачи **Обновление** приложение отправляет запросы серверам обновлений "Лаборатории Касперского".

Некоторые обновления требуют установки последних версий плагинов управляемых приложений.

О статусах обновлений

Статус – это атрибут обновлений программного обеспечения, который определяет, должны ли определенные обновления программного обеспечения быть установлены на сетевое устройство.

Обновление может иметь следующие статусы:

- *Не определено*.

  По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Неопределенные обновления могут быть установлены только на Агенте администрирования и других компонентах Kaspersky SIEM Cloud в соответствии с параметрами политики Агента администрирования.

- *Одобрено*.

  Одобренные обновления всегда устанавливаются. Если обновление требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения.

- *Отклонено.*

  Обновления, которым вы установили статус *Отклонено*, не устанавливаются на управляемые устройства.

Вы можете изменить статусы обновлений для следующих приложений:

- Агент администрирования и другие компоненты Kaspersky SIEM Cloud.

  По умолчанию загруженные обновления и патчи для компонентов Kaspersky SIEM Cloud устанавливаются автоматически. Если вы оставили включенным параметр **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"** в свойствах Агента администрирования, тогда все обновления будут установлены автоматически после их загрузки в хранилище (или несколько хранилищ). Если флажок снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.

  Обновления для компонентов Open Single Management Platform не могут быть удалены, даже если вы установите обновлениям статус *Отклонено*.

- Приложения безопасности "Лаборатории Касперского".

  По умолчанию обновления для управляемых приложений устанавливаются только после изменения статуса обновления на *Одобрено*. Если ранее отклоненное обновление для приложения безопасности было установлено, Open Single Management Platform попытается удалить обновления со всех устройств.

Одобрение и отклонение обновлений программного обеспечения

Параметры задачи установки обновлений могут требовать одобрения обновлений, которые должны быть установлены. Вы можете подтверждать обновления, которые необходимо установить, и отклонять обновления, которые не должны быть установлены.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом установить эти обновления на клиентские устройства.

Одобрение и отклонение обновлений доступно только для Агента администрирования и управляемых приложений, установленных на клиентских устройствах под управлением Windows и Linux. Бесшовное обновление Сервера администрирования, OSMP Console и веб-плагинов управления не поддерживается. Для обновления этих компонентов вам необходимо скачать их последние версии с сайта "Лаборатории Касперского" и установить их вручную.

Чтобы подтвердить или отменить одно или несколько обновлений:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Приложения "Лаборатории Касперского" → Бесшовные обновления**.

   Отобразится список доступных обновлений.

   Для обновлений управляемых приложений может потребоваться установка определенной минимальной версии Kaspersky Security Center. Если эта версия более поздняя, чем ваша текущая, эти обновления отображаются, но не могут быть одобрены. Также из таких обновлений невозможно создать инсталляционные пакеты, пока вы не обновите Kaspersky Security Center. Вам будет предложено обновить ваш экземпляр Kaspersky Security Center до необходимой минимальной версии.

2. При необходимости примите Лицензионное соглашение, нажав на кнопку **Просмотреть и принять Лицензионные соглашения**.

   Чтобы просмотреть данные, обрабатываемые приложениями "Лаборатории Касперского", для которых вы хотите подтвердить бесшовные обновления, нажмите **Просмотреть список данных** в открывшейся панели Лицензионное соглашение.

3. Выберите обновления, которые требуется подтвердить или отклонить.

4. Нажмите на кнопку **Одобрить**, чтобы одобрить выбранное обновление, или **Отклонить**, чтобы отклонить выбранное обновление.

   По умолчанию установлено значение *Не определено*.

Обновления, для которых вы установили статус *Одобрено*, помещаются в очередь на установку.

Обновления, для которых вы установили статус *Отклонено*, деинсталлируются (если это возможно) с устройств, на которые они были ранее установлены. Также они не будут установлены на устройства позже.

Некоторые обновления для приложений "Лаборатории Касперского" невозможно деинсталлировать. Если вы установили для них статус *Отклонено*, Kaspersky SIEM Cloud не будет деинсталлировать эти обновления с устройств, на которые они были установлены ранее. Такие обновления никогда не будут установлены на устройства в будущем.

Если вы устанавливаете статус *Отклонено* для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. Если вам потребуется удалить обновления, вы можете сделать это вручную локально.

Использование файлов различий для обновления баз и модулей приложений "Лаборатории Касперского".

Файл различий описывает различия между двумя версиями файлов базы или модулями приложений. Использование файлов различий уменьшает трафик внутри сети вашей организации, так как файлы различий занимают меньше места, чем целые файлы баз и модулей приложений. Если функция *Загрузить файлы различий* включена для точки распространения, то файлы различий сохраняются на этой точке распространения. В результате устройства, которые получают обновления от этой точки распространения, могут использовать сохраненные файлы различий для обновления своих баз и модулей приложений.

Для оптимизации использования файлов различий рекомендуется синхронизировать расписание обновления устройств с расписанием обновлений точки распространения, с которых это устройство получает обновления. Однако трафик может быть сохранен, даже если устройства обновляются в несколько раз реже, чем точка распространения, с которой устройство получает обновления.

Точки распространения не используют многоадресную IP-рассылку для автоматического распространения файлов различий.

Чтобы включить функцию загрузки файлов различий:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на имя задачи *Загрузка обновлений в хранилища точек распространения*, чтобы открыть свойства задачи.
3. На вкладке **Параметры приложения** включите параметр **Скачать файлы различий**.
4. Нажмите на кнопку **Сохранить**.

Функция загрузки файлов различий включена. Файлы различий обновлений загружаются в дополнение к файлам обновлений каждый раз, когда запускается задача *Загрузка обновлений в хранилища точек распространения*.

Чтобы проверить, что функция загрузки файлов различий успешно включена, вы можете измерить внутренний трафик до и после выполнения сценария.

Обновление баз и модулей приложений "Лаборатории Касперского" на автономных устройствах

Обновление баз и модулей приложений "Лаборатории Касперского" на управляемых устройствах является важной задачей для обеспечения защиты устройств от вирусов и других угроз. Администратор обычно настраивает регулярное обновление с помощью хранилищ точек распространения.

Когда вам необходимо обновить базы данных и модули приложений на устройстве (или группе устройств), которое не подключено точке распространения или интернету, вам необходимо использовать альтернативные источники обновлений, такие как FTP-сервер или локальная папка. В этом случае вам нужно доставить файлы необходимых обновлений с помощью запоминающего устройства, такого как флеш-накопитель или внешний жесткий диск.

Вы можете скопировать требуемые обновления из следующих источников:

- Точка распространения.

  Чтобы хранилище точки распространения содержало обновления, необходимые для приложения безопасности, установленного на автономном устройстве, по крайней мере на одном из управляемых сетевых устройств должна быть установлено это приложение безопасности. Это приложение должно быть настроено на получение обновлений из хранилища точки распространения с помощью задачи *Загрузка обновлений в хранилища точек распространения*.

- Любое устройство, на котором установлено такое же приложение безопасности и настроено получение обновлений из хранилища точки распространения или напрямую с серверов обновлений "Лаборатории Касперского".

Ниже приведен пример настройки обновлений баз и модулей приложений путем копирования их из хранилища точки распространения.

Чтобы обновить базы данных и модули приложений "Лаборатории Касперского" на автономных устройствах:

1. Подключите съемный диск к устройству, выполняющему роль точки распространения.

2. Скопируйте файлы обновлений на съемный диск.

   По умолчанию обновления хранятся по адресу: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\Updates.

3. На автономных устройствах настройте приложение безопасности (например, Kaspersky Endpoint Security для Windows) на получение обновлений из локальной папки или общего ресурса, такого как FTP-сервер или общая папка.

4. Скопируйте файлы обновлений со съемного диска в локальную папку или общий ресурс, который вы хотите использовать в качестве источника обновлений.

5. На автономном устройстве, на которое требуется установить обновления, запустите задачу обновления Kaspersky Endpoint Security для Windows.

После завершения задачи обновления базы данных и модули приложений "Лаборатории Касперского" будут обновлены на устройстве.

Управление сторонними приложениями и исполняемыми файлами на клиентских устройствах

В этом разделе описаны возможности Kaspersky SIEM Cloud связанные с управлением сторонних приложений и исполняемых файлов на клиентских устройствах.

Ограничения Системного администрирования

Возможности Системного администрирования имеют ряд ограничений, которые зависят от режима работы приложения Kaspersky Security Center Cloud Console, используемой по лицензии.

Следующие лицензии не поддерживают Системное администрирование:

- Kaspersky Endpoint Security для бизнеса Стандартный
- Kaspersky Security для виртуальных и облачных сред

Следующие лицензии поддерживают Системное администрирование:

- Kaspersky Endpoint Security для бизнеса Расширенный
- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Total Security для бизнеса
- Kaspersky Security для виртуальных и облачных сред Enterprise

В таблице ниже сравниваются ограничения пробной версии приложения Kaspersky Security Center Cloud Console для лицензий, не поддерживающих Системное администрирования, и для лицензий, поддерживающих Системное администрирование.

Ограничения Системного администрирования

Ограничение	Пробный режим	Коммерческая версия: лицензии, которые не поддерживают Системное администрирование	Коммерческая версия: лицензии, которые поддерживают Системное администрирование
Максимальное количество задач *Установка обновлений Центра обновления Windows* или задач *Закрытие уязвимостей*	4	4	0 (невозможно создавать задачи этих типов)
Максимальное количество задач *Установка требуемых обновлений и закрытие уязвимостей*	2	Не поддерживается	4
Максимальное количество правил во всех задачах *Установка требуемых обновлений и закрытие уязвимостей* на всех серверах, включая виртуальные	10	Не поддерживается	50
Максимальное количество обновлений программного обеспечения, которые могут одновременно иметь статус *Одобрено*, на всех серверах, включая виртуальные	100	Не поддерживается	1000
Максимальное количество обновлений программного обеспечения, которые можно вручную добавить в задачу, на всех серверах, включая виртуальные	500	1000	1000
Максимальное количество уязвимостей в приложениях, которые можно вручную добавить в задачу, на всех серверах, включая виртуальные	500	1000	1000

Доступность Системного администрирования в пробном и коммерческом режимах и при различных вариантах лицензирования

Доступность Системного администрирования в Kaspersky Security Center Cloud Console зависит от того, используете ли вы приложение в пробном или коммерческом режиме, а также от выбранного вами варианта лицензирования. Используйте таблицу, чтобы проверить какие возможности Системного администрирования доступны.

Системное администрирование	Пробный режим	Коммерческая версия: Kaspersky Endpoint Security для бизнеса Стандартный	Коммерческая версия: Kaspersky Endpoint Security для бизнеса Расширенный, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Total Security для бизнеса
Ручное закрытие уязвимостей в приложениях Microsoft на управляемых устройствах под управлением Windows Создание задачи *Закрытие уязвимостей*	✓	✓	—
Ручная установка обновлений программного обеспечения Microsoft на управляемые устройства под управлением Windows Установка обновлений приложений сторонних производителей с помощью задачи *Установка обновлений Центра обновления Windows*	—	✓	✓
Автоматическая установка обновлений приложений сторонних производителей на основе правил и закрытие уязвимостей в приложениях сторонних производителей Создание задачи *Установка требуемых обновлений и закрытие уязвимостей* и установка обновлений Добавление правил для установки обновлений	✓	—	✓

О приложениях сторонних производителей

Kaspersky SIEM Cloud может помочь вам обновить приложения сторонних производителей, установленные на клиентских устройствах, и закрыть уязвимости в приложениях сторонних производителей. Kaspersky SIEM Cloud может обновлять приложения сторонних производителей только с текущей версии до последней версии.

Список стороннего программного обеспечения обновляется динамически и может быть изменен. Вы можете проверить, возможно ли обновить приложения сторонних производителей, установленные на устройствах пользователей, с помощью Kaspersky SIEM Cloud, просмотрев список доступных обновлений в OSMP Console.

Процедура ниже предназначена для просмотра списка стороннего программного обеспечения, которое можно обновить с помощью Kaspersky SIEM Cloud. Для доступа к соответствующей информации без инициирования каких-либо задач необходимо выполнить описанные в процедуре действия.

Чтобы просмотреть список приложений сторонних производителей, которые можно обновить с помощью Kaspersky SIEM Cloud:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На шаге мастера **Параметры новой задачи** укажите следующие параметры:

   a. В раскрывающемся списке **Приложение** выберите **Kaspersky SIEM Cloud**.

   b. В поле **Тип задачи** выберите **Установка требуемых обновлений и закрытие уязвимостей**.

4. На шаге мастера **Область действия задачи** выберите параметр **Управляемые устройства**.
5. На шаге мастера **Задайте правила установки обновлений** нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.
6. На шаге мастера **Выбор типа правила** выберите параметр **Правило для сторонних обновлений**.
7. На шаге мастера **Общие критерии** выберите параметр **Устанавливать все обновления, кроме отклоненных** и нажмите на кнопку **Далее**.

Отобразится список приложений сторонних производителей.

Обновления приложений сторонних производителей

Kaspersky SIEM Cloud позволяет управлять обновлениями программного обеспечения сторонних производителей, установленных на управляемых устройствах, и закрывать уязвимости в приложениях Microsoft и других производителей программного обеспечения с помощью установки необходимых обновлений.

Kaspersky SIEM Cloud выполняет поиск обновлений с помощью задачи *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Сервер администрирования получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, указанных в свойствах задачи и установленных на устройствах. После просмотра информации о доступных обновлениях вы можете выполнить установку обновлений на устройства.

Обновление некоторых приложений Kaspersky SIEM Cloud выполняет путем удаления предыдущей версии приложения и установки новой версии.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных приложений с помощью технологий "Лаборатории Касперского". Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

Эксперты "Лаборатории Касперского" не проводят ручной анализ обновлений приложений сторонних производителей, которые можно установить с помощью Системного администрирования. Также эксперты "Лаборатории Касперского" не занимаются поиском уязвимостей (известных или неизвестных) или недокументированных возможностей в таких обновлениях и не проводят другие виды анализа упомянутых выше обновлений.

Задачи для установки обновлений приложений сторонних производителей

Когда метаданные обновлений приложений сторонних производителей загружаются в хранилище, вы можете установить обновления на клиентские устройства, выполнив следующие задачи:

- Задача *Установка требуемых обновлений и закрытие уязвимостей*.

Эта задача используется для установки обновлений для приложений Microsoft, включая обновления, предоставляемые службой Центра обновления Windows, и обновления приложений других поставщиков.

После завершения работы этой задачи обновления устанавливаются на управляемые устройства автоматически. При загрузке метаданных новых обновлений в хранилище Сервера администрирования Open Single Management Platform проверяет, соответствуют ли обновления критериям, указанным в правилах обновлений. Все новые обновления, которые соответствуют критериям, будут загружены и установлены автоматически при следующем запуске задачи.

- Задача *Установка обновлений Центра обновления Windows*

  Эта задача может использоваться только для установки обновлений Центра обновления Windows.

  После завершения работы этой задачи устанавливаются только те обновления, которые указаны в свойствах задачи. Позже, если вы хотите установить новые обновления, вам нужно добавить требуемые обновления в список обновлений существующей задачи или создать задачу *Установка обновлений Центра обновления Windows*.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

Сценарий: обновление приложений сторонних производителей

В этом разделе представлен сценарий обновления приложений сторонних производителей, установленных на клиентских устройствах. Приложения сторонних производителей включают в себя приложения от Microsoft и других поставщиков программного обеспечения. Обновления для приложений Microsoft предоставляются службой Центра обновления Windows.

Этапы

Обновление производителей состоит из следующих этапов:

1. **Поиск требуемых обновлений**

   Чтобы найти обновления приложений сторонних производителей, необходимые для управляемых устройств, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Open Single Management Platform получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, указанных в свойствах задачи и установленных на устройствах.

   Задача *Поиск уязвимостей и требуемых обновлений* автоматически создается в мастере первоначальной настройки Kaspersky Security Center Сервера администрирования. Если вы не запустили мастер, создайте задачу или запустите мастер первоначальной настройки.

   Инструкции:

   - Создание задачи Поиск уязвимостей и требуемых обновлений.
   - Параметры задачи поиска уязвимостей и требуемых обновлений.

2. **Анализ списка найденных обновлений**

   Просмотрите список **Обновления ПО** и решите, какие обновления следует установить. Чтобы просмотреть подробную информацию о каждом обновлении, нажмите на имя обновления в списке. Для каждого обновления в списке также можно просмотреть статистику установки обновлений на управляемых устройствах. Например, вы можете просмотреть количество устройств, на которых выбранное обновление не установлено, будет установлено или на которых не удалось установить обновление.

   Инструкции: Просмотр информации о доступных обновлениях приложений сторонних производителей.

3. **Настройка установки обновлений**

   После того как Open Single Management Platform получает список обновлений приложений сторонних производителей, вы можете установить их на клиентские устройства, используя задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. Создайте одну из этих задач. Вы можете создать эти задачи на вкладке **Задачи** или с помощью списка **Обновления ПО**.

   Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для установки обновлений для приложений Microsoft, включая обновления, предоставляемые службой Центра обновления Windows, и обновления приложений других поставщиков.

   Задача *Установка обновлений Центра обновления Windows* может использоваться только для установки обновлений Центра обновления Windows.

   Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

   Для установки некоторых обновлений программного обеспечения вам нужно принять Лицензионное соглашение для установки программного обеспечения. Если вы отклоните Лицензионное соглашение, обновления программного обеспечения не будут установлены.

   Инструкции:

   - Создание задачи Установка требуемых обновлений и закрытие уязвимостей.
   - Создание задачи Установка обновлений Центра обновления Windows.
   - Просмотр информации о доступных обновлениях приложений сторонних производителей.

4. **Задание расписания задачи**

   Чтобы убедится, что список обновлений всегда актуален, задайте расписание запуска задачи *Поиск уязвимостей и требуемых обновлений*, чтобы она периодически запускалась автоматически. По умолчанию период – один раз в неделю.

   Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью, что и для задачи *Поиск уязвимостей и требуемых обновлений*, или реже. При планировании задачи *Установка обновлений Центра обновления Windows* обратите внимание, что для этой задачи вам нужно определять список обновлений каждый раз перед запуском этой задачи.

   При задании расписания задач убедитесь, что задача закрытия уязвимостей запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

   Инструкции: Общие параметры задач.

5. **Одобрение и отклонение обновлений программного обеспечения (если требуется)**

   Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете указать правила установки обновлений в свойствах задачи. Если вы создали задачу *Установка обновлений Центра обновления Windows*, пропустите этот шаг.

Для каждого правила вы можете выбрать устанавливаемые обновления в зависимости от их статуса: *Не определено*, *Одобрено* или *Отклонено*. Например, вы можете создать определенную задачу для серверов и установить правило для этой задачи, чтобы разрешить установку только обновлений Центра обновления Windows и только тех, которые имеют статус *Одобрено*. После этого вы вручную устанавливаете статус *Одобрено* для тех обновлений, которые вы хотите установить. В этом случае обновления Центра обновления Windows со статусом *Не определено* или *Отклонено* не будут установлены на серверы, указанные в задаче.

По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус на *Одобрено* или *Отклонено* в списке **Обновления ПО** (**Управление программным обеспечением** → **Управление патчами** → **Обновления ПО**).

Инструкция: Одобрение и отклонение обновлений приложений сторонних производителей.

6. **Запуск задачи установки обновлений**

   Запустите задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. После запуска этих задач, обновления загружаются и устанавливаются на управляемые устройства. После завершения задачи убедитесь, что в списке задач она имеет статус *Завершена успешно*.

   Инструкция: Запуск задачи вручную.

7. **Создание отчета о результатах установки обновлений приложений сторонних производителей (если требуется)**

   Чтобы убедиться, что задача создана и обновления установлены, создайте **Отчет о результатах установки обновлений стороннего ПО** и просмотрите подробную статистику установки обновлений в этом отчете.

   Инструкция: Создание и просмотр отчета.

Установка обновлений приложений сторонних производителей

Вы можете установить обновления приложений сторонних производителей на управляемые устройства, создав и запустив одну из следующих задач:

- *Установка требуемых обновлений и закрытие уязвимостей*

  Эту задачу можно использовать для установки обновлений Центра обновления Windows, предоставленных Microsoft, и обновлений приложений других поставщиков.

- *Установка обновлений Центра обновления Windows*

  Эту задачу можно использовать только для установки обновлений Центра обновления Windows.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Также вы можете создать задачу для установки необходимых обновлений следующими способами:

- Открыть список обновлений и указать, какие обновления устанавливать.

  В результате создается задача для установки выбранных обновлений. Также вы можете добавить выбранные обновления в существующую задачу.

- Запустить мастер установки обновлений.

  > Доступность мастера установки обновлений зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии.

  Мастер упрощает создание и настройку задачи установки обновлений и позволяет исключить создание избыточных задач, содержащих те же самые обновления для установки.

Установка обновлений приложений сторонних производителей с помощью списка обновлений

Чтобы установить обновления приложений сторонних производителей:

1. Откройте один из списков обновлений:

   - Чтобы открыть список общих обновлений, в главном меню перейдите в раздел **Управление программным обеспечением → Управление патчами → Обновления ПО**.

   - Чтобы открыть список обновлений для управляемого устройства, в главном меню перейдите в раздел **Управление активами → Управляемые устройства → <имя устройства> → Дополнительно → Применимые обновления**.

   - Чтобы открыть список обновлений для определенного приложения, в главном меню перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Реестр приложений → <имя приложения> → Применимые обновления**.

   Отобразится список доступных обновлений.

2. Установите флажки рядом с теми обновлениями, которые вы хотите установить.

3. Нажмите на кнопку **Установить обновления**.

   Для установки некоторых обновлений программного обеспечения вам нужно принять Лицензионное соглашение. Если вы отклоните Лицензионное соглашение, обновления программного обеспечения не будут установлены.

4. Выберите один из следующих вариантов:

   - **Новая задача**

     Запустится мастер создания задачи. Задача *Установка требуемых обновлений и закрытие уязвимостей* или задача *Установка обновлений Центра обновления Windows* выбрана по умолчанию в зависимости от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии. Следуйте далее указаниям мастера, чтобы завершить создание задачи.

   - **Установить обновление (добавить правило в указанную задачу)**

Выберите задачу, в которую вы хотите добавить выбранные обновления. Выберите задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. Если вы выберите задачу *Установка требуемых обновлений и закрытие уязвимостей*, новое правило для установки выбранных обновлений автоматически добавится в выбранную задачу. Если вы выберете задачу *Установка обновлений Центра обновления Windows*, выбранные обновления будут добавлены в свойства задачи.

Откроется окно свойств задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы выбрали создание задачи, она создается и отображается в списке задач в разделе **Задачи**. Если вы выбрали добавление обновлений в существующую задачу, обновления сохраняются в свойствах задачи.

Чтобы установить обновления приложений сторонних производителей, запустите задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. Вы можете запустить эти задачи вручную или задать расписание в свойствах задачи, которую вы запускаете. При указании расписания задачи убедитесь, что задача установки обновления запускается после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

Установка обновлений приложений сторонних производителей с помощью мастера установки обновлений

Доступность этой функции зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии.

Чтобы создать задачу установки обновлений приложений сторонних производителей с помощью мастера установки обновления:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Управление патчами → Обновления ПО**.

   Отобразится список доступных обновлений.

2. Установите флажок рядом с обновлением, которое вы хотите установить.

3. Нажмите на кнопку **Запустить мастер установки обновления**.

   Запустится мастер установки обновления. На странице **Выбор задачи установки обновления** отображается список всех существующих задач следующих типов:

   - *Установка требуемых обновлений и закрытие уязвимостей*
   - *Установка обновлений Центра обновления Windows*
   - *Закрытие уязвимостей*

   Вы не можете изменить задачи двух последних типов для установки новых обновлений. Для установки новых обновлений можно использовать только задачи *Установка требуемых обновлений и закрытие уязвимостей*.

4. Если вы хотите, чтобы мастер отображал только те задачи, которые устанавливают выбранное вами обновление, включите параметр **Показать только задачи, которые устанавливают обновление**.

5. Выберите действие, которое хотите выполнить:

- Чтобы запустить задачу, установите флажок рядом с именем задачи и нажмите на кнопку **Запустить**.
- Чтобы добавить новое правило в существующую задачу:

  a. Установите флажок рядом с именем задачи и нажмите на кнопку **Добавить правило**.

  b. На открывшейся странице настройте новое правило:

  - **Правило установки обновлений данного уровня важности**

    Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

    Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение важности выбранного обновления (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

    Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

    По умолчанию параметр выключен.

  - **Правило установки обновлений данного уровня важности по MSRC** (доступно только для обновлений Центра обновления Windows)

    Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

    Если этот параметр включен (доступно только для обновлений Microsoft), обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

    Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

    По умолчанию параметр выключен.

  - **Правило установки обновлений данного поставщика** (доступно только для обновлений приложений сторонних производителей)

    Этот параметр доступен только для обновлений приложений сторонних производителей. Kaspersky Next XDR Expert устанавливает только те обновления, которые относятся к приложениям того же производителя, что и выбранное обновление. Отклоненные обновления и обновления приложений других производителей не устанавливаются.

    По умолчанию параметр выключен.

  - **Правило установки обновлений типа**
  - **Правило установки выбранного обновления**
  - **Одобрить выбранные обновления**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

- **Автоматически устанавливать все предыдущие обновления приложений, необходимые для установки выбранных обновлений**

  Включите этот параметр, если вы согласны с установкой промежуточных версий приложений, когда это необходимо, для установки выбранных обновлений.

  Если этот параметр выключен, устанавливаются только выбранные версии приложений. Выключите этот параметр, если вы хотите непосредственно обновить приложения, не пытаясь последовательно установить версии приложений. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

  Например, у вас на устройстве установлена версия 3 приложения, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

  По умолчанию параметр включен.

c. Нажмите на кнопку **Добавить**.

- Чтобы создать задачу:

  a. Нажмите на кнопку **Новая задача**.

  b. На открывшейся странице настройте новое правило:

  - **Правило установки обновлений данного уровня важности**

    Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

    Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение важности выбранного обновления (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

    Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

    По умолчанию параметр выключен.

  - **Правило установки обновлений данного уровня важности по MSRC** (доступно только для обновлений Центра обновления Windows)

    Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен (доступно только для обновлений Microsoft), обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

- **Правило установки обновлений данного поставщика** (доступно только для обновлений приложений сторонних производителей)

  Этот параметр доступен только для обновлений приложений сторонних производителей. Kaspersky Next XDR Expert устанавливает только те обновления, которые относятся к приложениям того же производителя, что и выбранное обновление. Отклоненные обновления и обновления приложений других производителей не устанавливаются.

  По умолчанию параметр выключен.

- **Правило установки обновлений типа**

- **Правило установки выбранного обновления**

- **Одобрить выбранные обновления**

  Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

  По умолчанию параметр выключен.

- **Автоматически устанавливать все предыдущие обновления приложений, необходимые для установки выбранных обновлений**

  Включите этот параметр, если вы согласны с установкой промежуточных версий приложений, когда это необходимо, для установки выбранных обновлений.

  Если этот параметр выключен, устанавливаются только выбранные версии приложений. Выключите этот параметр, если вы хотите непосредственно обновить приложения, не пытаясь последовательно установить версии приложений. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

  Например, у вас на устройстве установлена версия 3 приложения, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

  По умолчанию параметр включен.

c. Нажмите на кнопку **Добавить**.

Если вы решили запустить задачу, вы можете закрыть мастер. Задача выполняется в фоновом режиме. Никаких дальнейших действий не требуется.

Если вы выбрали добавление правила к существующей задаче, откроется окно свойств задачи. Новое правило уже добавлено в свойства задачи. Вы можете просмотреть или изменить правило, а также другие параметры задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы решили создать задачу, создайте ее с помощью мастера создания задачи. Новое правило, добавленное вами в мастере установки обновлений, отображается в мастере создания задачи. После завершения работы мастера задача *Установка требуемых обновлений и закрытие уязвимостей* добавлена в список задач.

Создание задачи Поиск уязвимостей и требуемых обновлений

С помощью задачи Поиск уязвимостей и требуемых обновлений Open Single Management Platform получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, установленных на управляемых устройствах.

Задача Поиск уязвимостей и требуемых обновлений создается автоматически во время работы мастера первоначальной настройки. Если вы не запускали мастер первоначальной настройки, вы можете создать задачу вручную.

Чтобы создать задачу Поиск уязвимостей и требуемых обновлений:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky SIEM Cloud выберите тип задачи **Поиск уязвимостей и требуемых обновлений**.
4. Укажите название задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите устройства, которым будет назначена задача.
6. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
7. Нажмите на кнопку **Создать**.

   Задача будет создана и отобразится в списке задач.
8. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
9. В окне свойств задачи укажите общие параметры задачи.
10. На вкладке **Параметры приложения** укажите следующие параметры:

    - **Поиск уязвимостей и обновлений, перечисленных Microsoft**

      При поиске уязвимостей и обновлений Kaspersky SIEM Cloud использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

      Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних приложений.

      По умолчанию параметр включен.

      Информация о необязательных обновлениях Microsoft Windows не отправляется на Сервер администрирования.

- **Соединяться с сервером обновлений для актуализации данных**

  Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft. Следующие службы могут выступать в качестве источника обновлений Microsoft:

  - Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
  - Серверы обновления Microsoft.

  Если этот параметр включен, Агент обновлений Windows на управляемом устройстве подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

  Если этот параметр выключен, Агент обновлений Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, которую он получил из источника обновлений Microsoft ранее.

  Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Вы можете выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах политики Агента администрирования, в разделе **Обновления и уязвимости в приложениях**. Если вы не хотите выключать этот параметр, то, чтобы уменьшить нагрузку на Сервер, вы можете настроить расписание задач так, чтобы использовать случайное значение задержки запуска задачи в интервале 360 минут.

  По умолчанию параметр включен.

  Комбинация следующих значений параметров политики Агента администрирования определяет режим получения обновлений:

  - Агент обновлений Windows на управляемом устройстве подключается к серверу обновлений для получения обновлений только в случае, если параметр **Соединяться с сервером обновлений для актуализации данных** включен в свойствах задачи *Поиск уязвимостей и требуемых обновлений* и параметр **Режим поиска Центра обновления Windows** установлен в **Активный** в параметрах политики Агента администрирования.
  - Если вам не требуется, чтобы Агент администрирования инициировал соединение с источником обновлений Microsoft Windows и загружал обновления при выполнении задачи *Поиск уязвимостей*, вы можете установить для параметра **Режим поиска Центра обновления Windows** значение **Пассивный**, при этом параметр **Соединяться с сервером обновлений для актуализации данных** должен оставаться включенным. Это позволяет сохранить ресурсы и использовать ранее полученные обновления Windows для поиска уязвимостей. Вы можете использовать пассивный режим, если настроили получение обновлений Microsoft Windows другим способом. Если получение обновлений Microsoft Windows не настроено по-другому, не устанавливайте для параметра **Режим поиска Центра обновления Windows** значение **Пассивный**, так как в этом случае информация об обновлениях никогда не будет получена.
  - Независимо от параметра **Соединяться с сервером обновлений для актуализации данных** (включен он или выключен), если для параметра **Выключен** выбрано значение **Режим поиска Центра обновления Windows**, Kaspersky SIEM Cloud не запрашивает информацию об обновлениях.

Если в сети вашей организации используется WSUS-сервер (локальный WSUS-сервер) и вы хотите использовать его вместе с Сервером администрирования Kaspersky Security Center, выполните следующие действия:

1. На управляемых устройствах с операционной системой Windows указать локальный WSUS-сервер для службы Центра обновления Windows. Вы можете сделать это вручную в реестре Windows или с помощью групповой политики Windows.

2. На локальном WSUS-сервере указать требуемые классификации для обновлений и приложений, по которым они будут распространяться.

3. Синхронизировать свой WSUS-сервер с вышестоящим сервером (это может быть либо Microsoft WSUS-сервер, либо другой локальный вышестоящий WSUS-сервер).

После запуска задачи *Поиск уязвимостей и требуемых обновлений* на устройстве Агент администрирования с помощью службы Центра обновления Windows инициирует запрос обновлений Windows, применимых к устройству. Служба Центра обновления Windows получает адрес внешнего WSUS-сервера из реестра и выполняет поиск обновлений непосредственно с этого внешнего WSUS-сервера. Затем служба Центра обновления Windows пересылает этот список на Сервер администрирования с помощью Агента администрирования. Таким образом, Сервер администрирования имеет актуальную базу.

- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

  Если этот параметр включен, Kaspersky SIEM Cloud выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите пути для дополнительного поиска приложений в файловой системе**. Полный список поддерживаемых приложений сторонних производителей контролируется "Лабораторией Касперского".

  Если этот параметр выключен, Kaspersky SIEM Cloud не выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних приложений.

  По умолчанию параметр включен.

- **Укажите пути для дополнительного поиска приложений в файловой системе**

  Папки, в которых Kaspersky SIEM Cloud выполняет поиск сторонних приложений, требующих закрытия уязвимостей и установки обновлений. Вы можете использовать системные переменные.

  Укажите папки, в которые были установлены приложения. По умолчанию список содержит системные папки, в которые устанавливается большинство приложений.

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать файлы трассировки, даже если запись файлов трассировки выключена для Агента администрирования в утилите удаленной диагностики Open Single Management Platform. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Open Single Management Platform. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

  По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

11. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

Если результаты задачи содержат предупреждение об ошибке 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

Параметры задачи поиска уязвимостей и требуемых обновлений

Задача *Поиск уязвимостей и требуемых обновлений* создается автоматически во время работы мастера первоначальной настройки. Если вы не запускали мастер первоначальной настройки, вы можете создать задачу вручную.

Помимо общих параметров задачи, вы можете указать следующие параметры при создании задачи *Поиск уязвимостей и требуемых обновлений* или позже, при настройке свойств созданной задачи:

- **Поиск уязвимостей и обновлений, перечисленных Microsoft**

  При поиске уязвимостей и обновлений Kaspersky SIEM Cloud использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

  Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних приложений.

  По умолчанию параметр включен.

  Информация о необязательных обновлениях Microsoft Windows не отправляется на Сервер администрирования.

- **Соединяться с сервером обновлений для актуализации данных**

  Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft. Следующие службы могут выступать в качестве источника обновлений Microsoft:

  - Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
  - Серверы обновления Microsoft.

Если этот параметр включен, Агент обновлений Windows на управляемом устройстве подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

Если этот параметр выключен, Агент обновлений Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, которую он получил из источника обновлений Microsoft ранее.

Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Вы можете выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах политики Агента администрирования, в разделе **Обновления и уязвимости в приложениях**. Если вы не хотите выключать этот параметр, то, чтобы уменьшить нагрузку на Сервер, вы можете настроить расписание задач так, чтобы использовать случайное значение задержки запуска задачи в интервале 360 минут.

По умолчанию параметр включен.

Комбинация следующих значений параметров политики Агента администрирования определяет режим получения обновлений:

- Агент обновлений Windows на управляемом устройстве подключается к серверу обновлений для получения обновлений только в случае, если параметр **Соединяться с сервером обновлений для актуализации данных** включен в свойствах задачи *Поиск уязвимостей и требуемых обновлений* и параметр **Режим поиска Центра обновления Windows** установлен в **Активный** в параметрах политики Агента администрирования.

- Если вам не требуется, чтобы Агент администрирования инициировал соединение с источником обновлений Microsoft Windows и загружал обновления при выполнении задачи *Поиск уязвимостей*, вы можете установить для параметра **Режим поиска Центра обновления Windows** значение **Пассивный**, при этом параметр **Соединяться с сервером обновлений для актуализации данных** должен оставаться включенным. Это позволяет сохранить ресурсы и использовать ранее полученные обновления Windows для поиска уязвимостей. Вы можете использовать пассивный режим, если настроили получение обновлений Microsoft Windows другим способом. Если получение обновлений Microsoft Windows не настроено по-другому, не устанавливайте для параметра **Режим поиска Центра обновления Windows** значение **Пассивный**, так как в этом случае информация об обновлениях никогда не будет получена.

- Независимо от параметра **Соединяться с сервером обновлений для актуализации данных** (включен он или выключен), если для параметра **Выключен** выбрано значение **Режим поиска Центра обновления Windows**, Kaspersky SIEM Cloud не запрашивает информацию об обновлениях.

Если в сети вашей организации используется WSUS-сервер (локальный WSUS-сервер) и вы хотите использовать его вместе с Сервером администрирования Kaspersky Security Center, выполните следующие действия:

1. На управляемых устройствах с операционной системой Windows указать локальный WSUS-сервер для службы Центра обновления Windows. Вы можете сделать это вручную в реестре Windows или с помощью групповой политики Windows.

2. На локальном WSUS-сервере указать требуемые классификации для обновлений и приложений, по которым они будут распространяться.

3. Синхронизировать свой WSUS-сервер с вышестоящим сервером (это может быть либо Microsoft WSUS-сервер, либо другой локальный вышестоящий WSUS-сервер).

После запуска задачи *Поиск уязвимостей и требуемых обновлений* на устройстве Агент администрирования с помощью службы Центра обновления Windows инициирует запрос обновлений Windows, применимых к устройству. Служба Центра обновления Windows получает адрес внешнего WSUS-сервера из реестра и выполняет поиск обновлений непосредственно с этого внешнего WSUS-сервера. Затем служба Центра обновления Windows пересылает этот список на Сервер администрирования с помощью Агента администрирования. Таким образом, Сервер администрирования имеет актуальную базу.

- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

  Если этот параметр включен, Kaspersky SIEM Cloud выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите пути для дополнительного поиска приложений в файловой системе**. Полный список поддерживаемых приложений сторонних производителей контролируется "Лабораторией Касперского".

  Если этот параметр выключен, Kaspersky SIEM Cloud не выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних приложений.

  По умолчанию параметр включен.

- **Укажите пути для дополнительного поиска приложений в файловой системе**

  Папки, в которых Kaspersky SIEM Cloud выполняет поиск сторонних приложений, требующих закрытия уязвимостей и установки обновлений. Вы можете использовать системные переменные.

  Укажите папки, в которые были установлены приложения. По умолчанию список содержит системные папки, в которые устанавливается большинство приложений.

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать файлы трассировки, даже если запись файлов трассировки выключена для Агента администрирования в утилите удаленной диагностики Open Single Management Platform. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Open Single Management Platform. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

  По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

Рекомендации по настройке расписания запуска задачи

При планировании расписания запуска задачи *Поиск уязвимостей и требуемых обновлений* убедитесь, что включены два параметра **Запускать пропущенные задачи** и **Использовать автоматическое определение случайного интервала между запусками задачи**.

По умолчанию задача *Поиск уязвимостей и требуемых обновлений* настроена на запуск вручную. Если регламент работы организации предусматривает выключение устройств в это время, то задача *Поиск уязвимостей и требуемых обновлений* будет запущена после включения устройства (утром следующего дня). Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на процессор и дисковую подсистему устройства. Следует настроить оптимальное расписание задачи исходя из принятого в организации регламента работы.

Создание задачи Установка требуемых обновлений и закрытие уязвимостей

Доступность задачи *Установка требуемых обновлений и закрытие уязвимостей* зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии.

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в приложениях сторонних производителей, в том числе в приложениях Microsoft, установленных на управляемых устройствах. Эта задача позволяет установить несколько обновлений и закрыть несколько уязвимостей в соответствии с определенными правилами.

Чтобы установить обновления или исправить уязвимости с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей*, вы можете выполнить одно из следующих действий:

- Запустите мастер установки обновлений или мастер закрытия уязвимостей.
- Создайте задачу *Установка требуемых обновлений и закрытие уязвимостей*.
- Добавьте правило для установки обновления в существующую задачу *Установка требуемых обновлений и закрытие уязвимостей*.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

Чтобы создать задачу Установка требуемых обновлений и закрытие уязвимостей:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky SIEM Cloud выберите тип задачи **Установка требуемых обновлений и закрытие уязвимостей**.
4. Укажите название задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

5. Выберите устройства, которым будет назначена задача.

6. Укажите правила для установки обновления, а затем следующие параметры:

- **Начинать установку в момент перезагрузки или выключения устройства**

  Если флажок установлен, установка обновления выполняется перед перезагрузкой или выключением устройства. В противном случае установка обновлений выполняется по расписанию.

  Установите этот флажок, если установка обновлений может повлиять на производительность устройств.

  По умолчанию параметр выключен.

- **Устанавливать требуемые общесистемные компоненты**

  Если флажок установлен, перед установкой обновления приложение автоматически устанавливает все общесистемные компоненты (пререквизиты), необходимые для установки этого обновления. Например, такими пререквизитами могут являться обновления операционной системы.

  Если этот параметр выключен, необходимо установить пререквизиты вручную.

  По умолчанию параметр выключен.

- **Разрешать установку новой версии приложения при обновлении**

  Если этот параметр включен, обновления можно устанавливать, только если это приведет к установке новой версии приложения.

  Если этот параметр выключен, приложение не обновляется. Можно позднее установить новые версии приложений вручную или с помощью другой задачи. Например, можно использовать этот параметр, если инфраструктура вашей компании не поддерживает новую версию приложения или если требуется проверить обновление в тестовой инфраструктуре.

  По умолчанию параметр включен.

  > После установки новой версии приложения может быть нарушена работа других приложений, установленных на клиентских устройствах и зависящих от работы обновляемой приложения.

- **Скачивать обновления на устройство, не устанавливая их**

  Если флажок установлен, приложение загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

  Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Скачать обновления для**.

  Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

  По умолчанию параметр выключен.

- **Скачать обновления для**

  Эта папка используется для загрузки обновлений сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать файлы трассировки, даже если запись файлов трассировки выключена для Агента администрирования в утилите удаленной диагностики Open Single Management Platform. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Open Single Management Platform. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

  По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

7. Укажите параметры перезагрузки операционной системы:

- **Не перезагружать устройство**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

  Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

  После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Время ожидания перед принудительным закрытием приложения в заблокированных сеансах через (мин)**

  Принудительное завершение работы приложений, когда устройство пользователя заблокировано (автоматически после периода неактивности или вручную).

  Если параметр включен, работа приложений на заблокированном устройстве принудительно прекращается по истечении времени, указанного в поле ввода.

  Если параметр выключен, работа приложений на заблокированном устройстве не прекращается.

  По умолчанию параметр выключен.

8. Если вы включите параметр **Завершение создания задачи** на странице **Открыть окно свойств задачи после ее создания**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

9. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.

10. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

11. В окне свойств задачи укажите общие параметры задачи в соответствии с вашими требованиями.

12. Нажмите на кнопку **Сохранить**.

    Задача создана и настроена.

Если результаты задачи содержат предупреждение об ошибке 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

Добавление правил для установки обновлений

Доступность этой функции зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии.

При установке обновлений программного обеспечения или закрытии уязвимостей в приложениях с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей* необходимо указать правила установки обновлений. Эти правила определяют обновления для установки и уязвимости к закрытию.

Точные параметры зависят от того, добавляете ли вы правило для всех обновлений Центра обновления Windows или для обновлений приложений сторонних производителей (то есть приложений производства не "Лаборатории Касперского" и не Microsoft). При добавлении правила для обновлений Центра обновления Windows или обновлений приложений сторонних производителей вы можете выбрать приложения и версии приложений, для которых вы хотите установить обновления. При добавлении правила для всех обновлений вы можете выбрать обновления, которые необходимо установить, и уязвимости, которые необходимо закрыть с помощью установки обновлений.

Вы можете добавить правило для установки обновлений следующими способами:

- Добавить правило при создании задачи Установка требуемых обновлений и закрытие уязвимостей.
- Добавить правило на вкладке **Параметры приложения** в окне свойств существующей задачи *Установка требуемых обновлений и закрытие уязвимостей*.
- С помощью мастера установки обновлений или мастера закрытия уязвимостей.

Чтобы добавить правило для всех обновлений:

1. Нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. На странице **Тип правила** выберите **Правило для всех обновлений**.

3. В окне **Общие критерии** в раскрывающемся списке укажите следующие параметры:

   - **Набор обновлений для установки**

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

     По умолчанию параметр выключен.

4. В окне **Обновления** выберите обновления для установки:

   - **Устанавливать все подходящие обновления**

     В этом случае будут установлены все обновления программного обеспечения, соответствующие критериям, указанным на шаге мастера **Общие критерии**. Выбрано по умолчанию.

   - **Устанавливать только обновления из списка**

     В этом случае будут установлены обновления только того программного обеспечения, которые вы выбираете вручную в списке. Этот список содержит все доступные обновления программного обеспечения.

     Например, вы можете задать обновления в следующих случаях: чтобы проверить установку обновлений в тестовом окружении, чтобы обновить только критически важные приложения или чтобы обновить только требуемые приложения.

   - **Автоматически устанавливать все предыдущие обновления приложений, необходимые для установки выбранных обновлений**

     Включите этот параметр, если вы согласны с установкой промежуточных версий приложений, когда это необходимо, для установки выбранных обновлений.

     Если этот параметр выключен, устанавливаются только выбранные версии приложений. Выключите этот параметр, если вы хотите непосредственно обновить приложения, не пытаясь последовательно установить версии приложений. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

     Например, у вас на устройстве установлена версия 3 приложения, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

     По умолчанию параметр включен.

5. В окне **Уязвимости** выберите уязвимости, которые будут закрыты с установкой указанного обновления:

   - **Закрывать все уязвимости, соответствующие остальным критериям**

     В этом случае будут закрыты все уязвимости в приложениях, соответствующие критериям, указанным на шаге мастера **Общие критерии**. Выбрано по умолчанию.

   - **Закрыть только уязвимости из списка**

     Закрывать только уязвимости, которые выбраны вручную в списке. Этот список содержит все обнаруженные уязвимости.

     Например, вы можете задать уязвимости в следующих случаях: чтобы проверить закрытие уязвимостей в тестовом окружении, чтобы закрыть уязвимости только в критически важных приложениях или чтобы закрыть уязвимости только в требуемых приложениях.

6. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

Чтобы добавить правило для обновлений Центра обновления Windows:

1. Нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. На странице **Тип правила** выберите **Правило для обновлений Windows Update**.

3. В окне **Общие условия** настройте следующие параметры:

   - **Набор обновлений для установки**

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.

     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.

     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

     По умолчанию параметр выключен.

   - **Закрывать уязвимости с уровнем критичности по MSRC, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

     По умолчанию параметр выключен.

4. В окне **Приложения** выберите приложения и версии приложений, для которых вы хотите установить обновления. По умолчанию выбраны все приложения.

5. В окне **Категории обновлений** выберите категории обновлений для установки. Эти категории такие же, как и в каталоге Центра обновления Microsoft. По умолчанию выбраны все категории.

6. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

Чтобы добавить правило для обновления приложений сторонних производителей:

1. Нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. На странице **Тип правила** выберите **Правило для сторонних обновлений**.

3. В окне **Общие условия** настройте следующие параметры:

   - **Набор обновлений для установки**

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

     По умолчанию параметр выключен.

4. В окне **Приложения** выберите приложения и версии приложений, для которых вы хотите установить обновления. По умолчанию выбраны все приложения.

5. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе Параметры, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

Создание задачи Установка обновлений Центра обновления Windows

Задача Установка обновлений Центра обновления Windows позволяет устанавливать обновления программного обеспечения, предоставляемые службой Центра обновления Windows, на клиентские устройства.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

Чтобы создать задачу Установка обновлений Центра обновления Windows:

1. В главном окне приложения перейдите в раздел **Управление активами → Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для приложения Kaspersky SIEM Cloud выберите тип задачи **Установка обновлений Центра обновления Windows**.
4. Укажите название задачи, которую вы создаете.

   Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите устройства, которым будет назначена задача.
6. Нажмите на кнопку **Добавить**.

   Откроется список обновлений.
7. Выберите обновления Центра обновлений Windows, которые вы хотите установить и нажмите на кнопку **OK**.
8. Укажите параметры перезагрузки операционной системы:

   - **Не перезагружать устройство**

     Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

   - **Перезагрузить устройство**

     В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

   - **Запрашивать у пользователя**

     На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

     По умолчанию выбран этот вариант.

   - **Повторять запрос каждые (мин)**

     Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

     По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

     Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

  После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать приложения в заблокированных сеансах**

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

9. Задайте параметры учетной записи:

   - **Учетная запись по умолчанию**

     Задача будет запускаться под той же учетной записью, под которой было установлено и запущено приложение, выполняющее эту задачу.

     По умолчанию выбран этот вариант.

   - **Задать учетную запись**

     В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

   - **Учетная запись**

     Учетная запись, от имени которой будет запускаться задача.

   - **Пароль**

     Пароль учетной записи, от имени которой будет запускаться задача.

10. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

11. Нажмите на кнопку **Готово**.

    Задача будет создана и отобразится в списке задач.

12. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

13. В окне свойств задачи укажите общие параметры задачи в соответствии с вашими требованиями.

14. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

Просмотр информации о доступных обновлениях приложений сторонних производителей.

Вы можете просмотреть список доступных обновлений для приложений сторонних производителей, включая программное обеспечение Microsoft, установленных на клиентских устройствах.

Чтобы просмотреть список доступных обновлений для приложений сторонних производителей, установленных на клиентских устройствах,

В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Управление патчами** → **Обновления ПО**.

Отобразится список доступных обновлений.

Вы можете указать фильтр для просмотра списка обновлений приложений. Нажмите на значок **Фильтр** ( ) в верхнем правом углу списка обновлений приложений для управления фильтром. Вы также можете выбрать один из предустановленных фильтров в раскрывающемся списке **Предустановленные фильтры** над списком уязвимостей в приложениях.

Чтобы просмотреть свойства обновления:

1. Нажмите на имя требуемого обновления программного обеспечения.
2. Откроется окно свойств обновления, в котором отображается следующая информация, сгруппированная по вкладкам:

   - **Общие**

     На этой вкладке отображаются общие сведения о выбранном обновлении:

     - Статус одобрения обновления (можно изменить вручную, выбрав новый статус в раскрывающемся списке).
     - Дата и время регистрации обновления.
     - Дата и время создания обновления.
     - Уровень важности обновления.
     - Требования к установке, предъявляемые обновлением.
     - Семейство приложений, к которому относится обновление.
     - Приложение, к которому применяется обновление.
     - Номер версии обновления.

- **Атрибуты**

  На этой вкладке отображается набор атрибутов, которые вы можете использовать для получения дополнительных сведений о выбранном обновлении. Этот набор различается в зависимости от того, кем выпущено обновление: Microsoft или сторонним производителем.

  На вкладке отображается следующая информация об обновлении Microsoft:

  - Уровень важности обновления в соответствии Microsoft Security Response Center (MSRC).
  - Ссылка на статью в базе знаний Microsoft с описанием обновления.
  - Ссылка на статью в бюллетене Microsoft Security Bulletin с описанием обновления.
  - Идентификатор обновления (ID).

  На вкладке отображается следующая информация для обновления стороннего производителя:

  - Является ли обновление патчем или полным дистрибутивом.
  - Язык локализации обновления.
  - Устанавливается ли обновление автоматически или вручную.
  - Было ли обновление отозвано после применения.
  - Ссылка для загрузки обновления.

- **Устройства**

  На этой вкладке отображается список устройств, на которых установлено выбранное обновление.

- **Закрываемые уязвимости**

  На этой вкладке отображается список уязвимостей, которые выбранное обновление может закрыть.

- **Пересечения обновлений**

  На этой вкладке отображаются возможные пересечения между различными обновлениями, опубликованными для одного и того же приложения, то есть может ли выбранное обновление заменять другие обновления или, наоборот, можно ли его заменять другими обновлениями (доступно только для обновлений Microsoft).

- **Задачи для установки обновления**

  На этой вкладке отображается список задач, в область действия которых входит установка выбранного обновления. На вкладке также можно создать задачу удаленной установки обновления.

Чтобы просмотреть статистику установки обновления:

1. Установите флажок рядом с требуемым обновлением.
2. Нажмите на кнопку **Статистика состояния установки обновлений**.

На диаграмме отобразится информация о статусах обновлений. Нажав на статус, откроется список устройств, на которых обновление имеет выбранный статус.

Вы можете просмотреть информацию о доступных обновлениях для приложений сторонних производителей, включая программное обеспечение Microsoft, установленных на выбранном управляемом устройстве под управлением Windows.

Чтобы просмотреть список доступных обновлений для приложений сторонних производителей, установленных на выбранном управляемом устройстве:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием устройства, для которого вы хотите просмотреть обновления приложений сторонних производителей.

   Откроется окно свойств выбранного устройства.

3. В окне свойств выбранного устройства выберите вкладку **Дополнительно**.

4. На левой панели выберите раздел **Применимые обновления**. Если вы хотите просматривать только установленные обновления, включите параметр **Показывать установленные обновления**.

Отобразится список доступных обновлений приложений сторонних производителей для выбранного устройства.

Экспорт списка доступных обновлений в файл

Вы можете экспортировать список обновлений для приложений сторонних производителей, включая приложения Microsoft, в файл формата CSV или TXT. Вы можете использовать эти файлы, например, чтобы отправить их вашему начальнику по информационной безопасности или сохранить их в целях статистики.

Чтобы экспортировать список доступных обновлений для приложений сторонних производителей в текстовый файл, установленных на всех управляемых устройствах:

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Обновления ПО**.

   Отобразится список доступных обновлений.

   При экспорте полного списка обновлений приложений, будут экспортированы только те обновления, которые отображаются на текущей странице.

   Если вы хотите экспортировать только определенные обновления, установите флажки рядом с требуемыми обновлениями в списке.

2. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать. Если какая-либо из этих кнопок не отображается, нажмите на кнопку с многоточием и выберите нужный вариант в раскрывающемся списке.

Файл, содержащий список доступных обновлений для приложений сторонних производителей, включая приложения Microsoft, загружается на ваше текущее устройство.

Чтобы экспортировать список доступных обновлений для приложений сторонних производителей в текстовый файл, установленных на выбранном управляемом устройстве:

1. Откройте список доступных обновлений приложений сторонних производителей на выбранном управляемом устройстве.

   Отобразится список доступных обновлений.

При экспорте полного списка обновлений приложений, будут экспортированы только те обновления, которые отображаются на текущей странице.

Если вы хотите экспортировать только определенные обновления, установите флажки рядом с требуемыми обновлениями в списке.

Если вы хотите экспортировать только установленные обновления, установите флажок **Показывать установленные обновления**.

2. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать. Если какая-либо из этих кнопок не отображается, нажмите на кнопку с многоточием и выберите нужный вариант в раскрывающемся списке.

Файл, содержащий список доступных обновлений для приложений сторонних производителей, включая приложения Microsoft, установленные на выбранных управляемых устройствах, загружается на ваше текущее устройство.

Одобрение и отклонение обновлений приложений сторонних производителей.

При настройке задачи *Установка требуемых обновлений и закрытие уязвимостей*, вы можете создать правило, для выполнения которого устанавливаемые обновления должны иметь определенный статус. Например, правило обновления может разрешить установку следующего:

- только одобренных обновлений;
- только одобренных обновлений и неопределенных обновлений;
- всех обновлений, независимо от статусов обновлений.

Вы можете подтверждать обновления, которые необходимо установить, и отклонять обновления, которые не должны быть установлены.

При управлении установкой обновлений использовать статус *Одобрено* целесообразно для небольшого количества обновлений. Чтобы установить несколько обновлений, используйте правила, которые вы можете настроить в задаче *Установка требуемых обновлений и закрытие уязвимостей*. Рекомендуется устанавливать статус *Одобрено* только для тех обновлений, которые не соответствуют критериям, указанным в правилах. При ручном одобрении большого количества обновлений производительность Сервера администрирования снижается, что может привести к перегрузке Сервера администрирования.

Чтобы подтвердить или отменить одно или несколько обновлений:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Управление патчами** → **Обновления ПО**.

   Отобразится список доступных обновлений.

2. Выберите обновления, которые требуется подтвердить или отклонить.

3. Нажмите на кнопку **Одобрить**, чтобы одобрить выбранное обновление, или **Отклонить**, чтобы отклонить выбранное обновление.

   По умолчанию установлено значение *Не определено*.

Выбранные обновления имеют статусы, которые вы указали.

Также вы можете изменить статус в свойствах требуемого обновления.

Чтобы одобрить или отклонить обновление:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Управление патчами** → **Обновления ПО**.

   Отобразится список доступных обновлений.

2. Выберите обновление, которое требуется одобрить или отклонить.

   Откроется окно свойств обновления.

3. В разделе **Общие** выберите статус обновления, изменив параметр **Статус одобрения обновления**. Вы можете выбрать статус *Одобрено*, *Отклонено* или *Не определено*.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Выбранное обновление имеет статус, который вы указали.

Если вы устанавливаете статус **Отклонено** для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. Если вам потребуется удалить их, вы можете сделать это вручную локально.

Автоматическое обновление приложений сторонних производителей

Некоторые приложения сторонних производителей могут обновляться автоматически. Поставщик приложения определяет, поддерживает ли приложение функцию автоматического обновления. Если приложение стороннего производителя, установленное на управляемом устройстве, поддерживает автоматическое обновление, вы можете указать параметр автоматического обновления в свойствах приложения. После изменения параметра автоматического обновления Агенты администрирования применяют новый параметр на каждом управляемом устройстве, на котором установлено приложение.

Параметр автоматического обновления не зависит от других объектов и возможностей Системного администрирования. Например, этот параметр не зависит от статуса одобрения обновления или задач установки обновления, таких как *Установка требуемых обновлений и закрытие уязвимостей*, *Установка обновлений Центра обновления Windows* и *Закрытие уязвимостей*.

Чтобы настроить параметр автоматического обновления для приложения стороннего производителя:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Сторонние приложения** → **Реестр приложений**.

2. Нажмите на имя приложения, для которого вы хотите изменить параметр автоматического обновления.

   Чтобы упростить поиск, вы можете отфильтровать список по столбцу **Статус автоматических обновлений**.

   Откроется окно свойств приложения.

3. В разделе **Общие** выберите значение для следующего параметра:

   Статус автоматических обновлений

Выберите один из следующих вариантов:

- **Не определено**

  Функция автоматического обновления выключена. Open Single Management Platform устанавливает обновления приложений сторонних производителей с помощью задач: *Установка требуемых обновлений и закрытие уязвимостей* и *Закрытие уязвимостей*.

- **Разрешено**

  После того как поставщик выпускает обновление для приложения, это обновление автоматически устанавливается на управляемые устройства. Никаких дополнительных действий не требуется.

- **Заблокировано**

  Обновления приложения не устанавливаются автоматически. Open Single Management Platform устанавливает обновления приложений сторонних производителей с помощью задач: *Установка требуемых обновлений и закрытие уязвимостей* и *Закрытие уязвимостей*.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Настройка автоматического обновления применяется к выбранному приложению.

Обнаружение и закрытие уязвимостей в приложениях

Kaspersky SIEM Cloud обнаруживает и закрывает уязвимости в приложениях на управляемых устройствах под управлением операционных систем семейства Microsoft Windows. Уязвимости обнаруживаются в операционной системе и в стороннем программном обеспечении, включая программное обеспечение Microsoft.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в приложении на территории США.

Обнаружение уязвимостей в приложениях

Для обнаружения уязвимостей Kaspersky SIEM Cloud выполняет поиск известных уязвимостей программного обеспечения на основе признаков из баз данных об известных уязвимостях и базы данных Центра обновления Windows. База данных об известных уязвимостях формируется и поддерживается специалистами "Лаборатории Касперского". Она содержит информацию об уязвимостях, такую как описание уязвимостей, дата обнаружения уязвимостей, уровень критичности уязвимостей. Информация об уязвимостях приложений приведена на сайте "Лаборатории Касперского".

В Kaspersky SIEM Cloud для поиска уязвимостей в приложениях используется задача *Поиск уязвимостей и требуемых обновлений*.

Закрытие уязвимостей в приложениях

Для закрытия уязвимостей в приложениях, Kaspersky SIEM Cloud использует обновления программного обеспечения выпущенные поставщиками программного обеспечения. Вы можете просмотреть список уязвимостей в приложениях в любое время. Метаданные обновлений программного обеспечения автоматически загружаются в хранилище Сервера администрирования и хранилища точек распространения в результате выполнения задачи *Загрузка обновлений в хранилища точек распространения*. Вы можете создать эту задачу с помощью мастера первоначальной настройки Kaspersky Security Center Cloud Console или вручную.

Обновления программного обеспечения для закрытия уязвимостей могут быть представлены в виде полных дистрибутивов или патчей. Обновления программного обеспечения, которые закрывают уязвимости программного обеспечения, называются *исправлениями*. В Kaspersky Security Center Cloud Console вы закрываете уязвимости, используя *рекомендуемые исправления*. Рекомендуемые исправления это обновления программного обеспечения, которые рекомендуются к установке специалистами "Лаборатории Касперского".

В зависимости от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии вы можете использовать задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Закрытие уязвимостей* для закрытия уязвимостей в приложениях.

Задача *Установка требуемых обновлений и закрытие уязвимостей* автоматически закрывает несколько уязвимостей, устанавливая рекомендуемые исправления. Для этой задачи вы можете вручную настроить определенные правила для закрытия нескольких уязвимостей.

С помощью задачи *Закрытие уязвимостей*, вы можете закрыть уязвимости, установив рекомендуемые исправления для программного обеспечения Microsoft.

Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных приложений с помощью технологий "Лаборатории Касперского". Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

Эксперты "Лаборатории Касперского" не проводят ручной анализ обновлений приложений сторонних производителей, которые можно установить с помощью Системного администрирования. Также эксперты "Лаборатории Касперского" не занимаются поиском уязвимостей (известных или неизвестных) или недокументированных возможностей в таких обновлениях и не проводят другие виды анализа упомянутых выше обновлений.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Для закрытия некоторых уязвимостей программного обеспечения вам нужно принять Лицензионное соглашение для установки программного обеспечения, если это требуется. Если вы отклоняете Лицензионное соглашение, уязвимость в программном обеспечении не может быть закрыта.

Информация о каждой закрытой уязвимости хранится на Сервере администрирования 90 дней. По истечении этого срока информация удаляется автоматически.

Закрытие уязвимостей в приложениях

После получения списка уязвимостей в приложениях вы можете закрыть уязвимости в приложениях на управляемых устройствах с операционными системами Windows. Вы можете закрыть уязвимости в операционной системе и приложениях сторонних производителей, включая программное обеспечение Microsoft, создав и запустив задачу *Закрытие уязвимостей* или задачу *Установка требуемых обновлений и закрытие уязвимостей*.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Также вы можете создать задачу для закрытия уязвимостей в приложениях следующими способами:

- Откройте список уязвимостей и укажите, какие уязвимости необходимо закрыть.

  В результате создается задача закрытия уязвимостей в приложениях. Также можно добавить выбранные уязвимости в существующую задачу.

- Запустите мастер закрытия уязвимостей.

  Доступность этой функции зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии.

  Мастер упрощает создание и настройку задачи закрытия уязвимостей, а также исключает создание избыточных задач, содержащих те же обновления для установки.

Закрытие уязвимостей в приложениях с помощью списка уязвимостей

Чтобы закрыть уязвимости в приложениях:

1. Откройте один из списков уязвимостей:

   - Чтобы открыть общий список уязвимостей, в главном меню перейдите в раздел **Управление программным обеспечением → Управление патчами → Уязвимости в приложениях**.

   - Чтобы открыть список уязвимостей управляемого устройства, в главном меню перейдите в раздел **Управление активами → Управляемые устройства → имя устройства → Дополнительно → Уязвимости в приложениях**.

   - Чтобы открыть список уязвимостей для требуемого приложения, в главном меню перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Реестр приложений → имя приложения → Уязвимости**.

   Отобразится страница со списком уязвимостей в приложениях сторонних производителей.

2. Выберите одну или несколько уязвимостей в списке и нажмите на кнопку **Закрыть уязвимость**.

   Если рекомендуемое обновление программного обеспечения для закрытия одной из выбранных уязвимостей отсутствует, отображается информационное сообщение.

   Для закрытия некоторых уязвимостей программного обеспечения вам нужно принять Лицензионное соглашение для установки программного обеспечения, если это требуется. Если вы отклоняете Лицензионное соглашение, уязвимость в программном обеспечении не закроется.

3. Выберите один из следующих вариантов:

   - **Новая задача**

     Запустится мастер создания задачи. В зависимости от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии, по умолчанию выбрана задача *Установка требуемых обновлений и закрытие уязвимостей* или задача *Закрытие уязвимостей*. Следуйте далее указаниям мастера, чтобы завершить создание задачи.

   - **Закрыть уязвимость (добавить правило в указанную задачу)**

     Выберите задачу, в которую вы хотите добавить выбранные уязвимости. В зависимости от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии выберите задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Закрытие уязвимостей*. В выбранную задачу *Установка требуемых обновлений и закрытие уязвимостей* автоматически добавится новое правило для закрытия выбранных уязвимостей. Если вы выберете задачу *Закрытие уязвимостей*, выбранные уязвимости будут добавлены в свойства задачи.

     Откроется окно свойств задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   Если вы выбрали создание задачи, она создается и отображается в списке задач в разделе **Задачи**. Если вы выбрали добавление уязвимостей в существующую задачу, уязвимости сохраняются в свойствах задачи.

Чтобы закрыть уязвимости в приложениях сторонних производителей, запустите задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Закрытие уязвимостей*. Если вы создали задачу *Закрытие уязвимостей*, вам нужно вручную указать обновления программного обеспечения для закрытия уязвимостей, перечисленных в свойствах задачи.

Закрытие уязвимостей в приложениях с помощью мастера закрытия уязвимостей

Доступность мастера закрытия уязвимостей зависит от действующей лицензии и режима работы Kaspersky Security Center Cloud Console.

Чтобы закрыть уязвимости в приложениях с помощью мастера закрытия уязвимостей:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Управление патчами** → **Уязвимости в приложениях**.

   Откроется страница со списком уязвимостей в приложениях сторонних производителей, установленных на управляемых устройствах.

2. Установите флажок напротив уязвимости, которую требуется закрыть.

3. Нажмите на кнопку **Запустить мастер закрытия уязвимости**.

   Откроется мастер закрытия уязвимости. На странице **Выбор задачи закрытия уязвимости** отображается список всех существующих задач следующих типов:

   - *Установка требуемых обновлений и закрытие уязвимостей*
   - *Установка обновлений Центра обновления Windows*
   - *Закрытие уязвимостей*

   Вы не можете изменить последние два типа задач для установки новых обновлений. Для установки новых обновлений можно использовать только задачу *Установка требуемых обновлений и закрытие уязвимостей*.

4. Если вы хотите, чтобы мастер отображал только те задачи, которые закрывают выбранную уязвимость, включите параметр **Показывать только задачи, которые закрывают выбранную уязвимость**.

5. Выберите действие, которое хотите выполнить:

   - Чтобы запустить задачу, установите флажок рядом с именем задачи и нажмите на кнопку **Запустить**.
   - Чтобы добавить новое правило в существующую задачу:

     a. Установите флажок рядом с именем задачи и нажмите на кнопку **Добавить правило**.

     b. На открывшейся странице настройте новое правило:

     - **Правило закрытия уязвимостей данного уровня критичности**

       Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

       Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение важности выбранного обновления (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

- **Правило для закрытия уязвимостей с помощью обновлений того же типа, что и обновление, определенное в соответствии с рекомендациями для выбранной уязвимости** (доступно только для уязвимостей в приложениях Microsoft)

- **Правило закрытия уязвимостей в приложениях выбранного поставщика** (доступно только для уязвимостей в приложениях сторонних производителей)

- **Правило закрытия уязвимости во всех версиях выбранного приложения** (доступно только для уязвимостей в приложениях сторонних производителей)

- **Правило закрытия выбранной уязвимости**

- **Одобрить обновления, закрывающие выбранную уязвимость**

  Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

  По умолчанию параметр выключен.

c. Нажмите на кнопку **Добавить**.

- Чтобы создать задачу:

  a. Нажмите на кнопку **Новая задача**.

  b. На открывшейся странице настройте новое правило:

  - **Правило закрытия уязвимостей данного уровня критичности**

    Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

    Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение важности выбранного обновления (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

    Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

    По умолчанию параметр выключен.

  - **Правило закрытия уязвимости с помощью обновлений типа** (доступно только для уязвимостей в приложениях Microsoft)

  - **Правило закрытия уязвимостей в приложениях выбранного поставщика** (доступно только для уязвимостей в приложениях сторонних производителей)

  - **Правило закрытия уязвимости во всех версиях выбранного приложения** (доступно только для уязвимостей в приложениях сторонних производителей)

- **Правило закрытия выбранной уязвимости**
- **Одобрить обновления, закрывающие выбранную уязвимость**

  Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

  По умолчанию параметр выключен.

c. Нажмите на кнопку **Добавить**.

Если вы решили запустить задачу, вы можете закрыть мастер. Задача выполняется в фоновом режиме. Никаких дальнейших действий не требуется.

Если вы выбрали добавление правила к существующей задаче, откроется окно свойств задачи. Новое правило уже добавлено в свойства задачи. Вы можете просмотреть или изменить правило, а также другие параметры задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы решили создать задачу, создайте ее с помощью мастера создания задачи. Новое правило, добавленное вами в мастер закрытия уязвимостей, отображается в мастере создания задачи. После завершения работы мастера создания задачи, задача *Установка требуемых обновлений и закрытие уязвимостей* добавлена в список задач.

Создание задачи Закрытие уязвимостей

Задача *Закрытие уязвимостей* позволяет закрыть уязвимости в приложениях Microsoft на управляемых устройствах с операционными системами Windows.

Доступность этой функции зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии. Рекомендуется использовать задачу *Установка требуемых обновлений и закрытие уязвимостей* вместо задачи *Закрытие уязвимостей*. Задача *Установка требуемых обновлений и закрытие уязвимостей* позволяет автоматически устанавливать несколько обновлений и закрывать несколько уязвимостей в соответствии с заданными правилами.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Чтобы создать задачу Закрытие уязвимостей:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для приложения Kaspersky SIEM Cloud выберите тип задачи **Закрытие уязвимостей**.

4. Укажите название задачи, которую вы создаете.

   Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

5. Выберите устройства, которым будет назначена задача.

6. Нажмите на кнопку **Добавить**.

   Откроется список уязвимостей.

7. Выберите уязвимости, которые вы хотите закрыть и нажмите на кнопку **OK**.

8. Укажите параметры перезагрузки операционной системы:

   - **Не перезагружать устройство**

     Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

   - **Перезагрузить устройство**

     В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

   - **Запрашивать у пользователя**

     На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

     По умолчанию выбран этот вариант.

   - **Повторять запрос каждые (мин)**

     Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

     По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

     Если параметр выключен, предложение перезагрузки отображается только один раз.

   - **Принудительно перезагрузить через (мин)**

     После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

     По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

   - **Принудительно закрывать приложения в заблокированных сеансах**

     Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

Если этот параметр включен, такие приложения на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

9. Задайте параметры учетной записи:

   - **Учетная запись по умолчанию**

     Задача будет запускаться под той же учетной записью, под которой было установлено и запущено приложение, выполняющее эту задачу.

     По умолчанию выбран этот вариант.

   - **Задать учетную запись**

     В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

   - **Учетная запись**

     Учетная запись, от имени которой будет запускаться задача.

   - **Пароль**

     Пароль учетной записи, от имени которой будет запускаться задача.

10. Если вы включите параметр **Завершение создания задачи** на странице **Открыть окно свойств задачи после ее создания**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

11. Нажмите на кнопку **Готово**.

    Задача будет создана и отобразится в списке задач.

12. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

13. В окне свойств задачи укажите общие параметры задачи в соответствии с вашими требованиями.

14. Нажмите на кнопку **Сохранить**.

    Задача создана и настроена.

Создание задачи Установка требуемых обновлений и закрытие уязвимостей

Доступность задачи *Установка требуемых обновлений и закрытие уязвимостей* зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии.

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в приложениях сторонних производителей, в том числе в приложениях Microsoft, установленных на управляемых устройствах. Эта задача позволяет установить несколько обновлений и закрыть несколько уязвимостей в соответствии с определенными правилами.

Чтобы установить обновления или исправить уязвимости с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей*, вы можете выполнить одно из следующих действий:

- Запустите мастер установки обновлений или мастер закрытия уязвимостей.
- Создайте задачу *Установка требуемых обновлений и закрытие уязвимостей*.
- Добавьте правило для установки обновления в существующую задачу *Установка требуемых обновлений и закрытие уязвимостей*.

Задачи установки обновлений программного обеспечения имеют ряд ограничений. Эти ограничения зависят от типа лицензии, по которой используется приложение Kaspersky Security Center Cloud Console, и от режима работы Kaspersky Security Center Cloud Console.

Чтобы создать задачу Установка требуемых обновлений и закрытие уязвимостей:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky SIEM Cloud выберите тип задачи **Установка требуемых обновлений и закрытие уязвимостей**.
4. Укажите название задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите устройства, которым будет назначена задача.
6. Укажите правила для установки обновления, а затем следующие параметры:

   - **Начинать установку в момент перезагрузки или выключения устройства**

     Если флажок установлен, установка обновления выполняется перед перезагрузкой или выключением устройства. В противном случае установка обновлений выполняется по расписанию.

     Установите этот флажок, если установка обновлений может повлиять на производительность устройств.

     По умолчанию параметр выключен.

   - **Устанавливать требуемые общесистемные компоненты**

     Если флажок установлен, перед установкой обновления приложение автоматически устанавливает все общесистемные компоненты (пререквизиты), необходимые для установки этого обновления. Например, такими пререквизитами могут являться обновления операционной системы.

     Если этот параметр выключен, необходимо установить пререквизиты вручную.

     По умолчанию параметр выключен.

- **Разрешать установку новой версии приложения при обновлении**

  Если этот параметр включен, обновления можно устанавливать, только если это приведет к установке новой версии приложения.

  Если этот параметр выключен, приложение не обновляется. Можно позднее установить новые версии приложений вручную или с помощью другой задачи. Например, можно использовать этот параметр, если инфраструктура вашей компании не поддерживает новую версию приложения или если требуется проверить обновление в тестовой инфраструктуре.

  По умолчанию параметр включен.

  > После установки новой версии приложения может быть нарушена работа других приложений, установленных на клиентских устройствах и зависящих от работы обновляемой приложения.

- **Скачивать обновления на устройство, не устанавливая их**

  Если флажок установлен, приложение загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

  Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Скачать обновления для**.

  Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

  По умолчанию параметр выключен.

- **Скачать обновления для**

  Эта папка используется для загрузки обновлений сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать файлы трассировки, даже если запись файлов трассировки выключена для Агента администрирования в утилите удаленной диагностики Open Single Management Platform. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Open Single Management Platform. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

  По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

7. Укажите параметры перезагрузки операционной системы:

- **Не перезагружать устройство**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

  Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

  По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

  Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

  После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Время ожидания перед принудительным закрытием приложения в заблокированных сеансах через (мин)**

  Принудительное завершение работы приложений, когда устройство пользователя заблокировано (автоматически после периода неактивности или вручную).

  Если параметр включен, работа приложений на заблокированном устройстве принудительно прекращается по истечении времени, указанного в поле ввода.

  Если параметр выключен, работа приложений на заблокированном устройстве не прекращается.

  По умолчанию параметр выключен.

8. Если вы включите параметр **Завершение создания задачи** на странице **Открыть окно свойств задачи после ее создания**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

9. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.

10. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

11. В окне свойств задачи укажите общие параметры задачи в соответствии с вашими требованиями.

12. Нажмите на кнопку **Сохранить**.

    Задача создана и настроена.

Если результаты задачи содержат предупреждение об ошибке 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

Добавление правил для установки обновлений

Доступность этой функции зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии.

При установке обновлений программного обеспечения или закрытии уязвимостей в приложениях с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей* необходимо указать правила установки обновлений. Эти правила определяют обновления для установки и уязвимости к закрытию.

Точные параметры зависят от того, добавляете ли вы правило для всех обновлений Центра обновления Windows или для обновлений приложений сторонних производителей (то есть приложений производства не "Лаборатории Касперского" и не Microsoft). При добавлении правила для обновлений Центра обновления Windows или обновлений приложений сторонних производителей вы можете выбрать приложения и версии приложений, для которых вы хотите установить обновления. При добавлении правила для всех обновлений вы можете выбрать обновления, которые необходимо установить, и уязвимости, которые необходимо закрыть с помощью установки обновлений.

Вы можете добавить правило для установки обновлений следующими способами:

- Добавить правило при создании задачи Установка требуемых обновлений и закрытие уязвимостей.
- Добавить правило на вкладке **Параметры приложения** в окне свойств существующей задачи *Установка требуемых обновлений и закрытие уязвимостей*.
- С помощью мастера установки обновлений или мастера закрытия уязвимостей.

Чтобы добавить правило для всех обновлений:

1. Нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. На странице **Тип правила** выберите **Правило для всех обновлений**.

3. В окне **Общие критерии** в раскрывающемся списке укажите следующие параметры:

- **Набор обновлений для установки**

  Выберите обновления, которые должны быть установлены на клиентские устройства:

  - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.

  - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.

  - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

  По умолчанию параметр выключен.

4. В окне **Обновления** выберите обновления для установки:

- **Устанавливать все подходящие обновления**

  В этом случае будут установлены все обновления программного обеспечения, соответствующие критериям, указанным на шаге мастера **Общие критерии**. Выбрано по умолчанию.

- **Устанавливать только обновления из списка**

  В этом случае будут установлены обновления только того программного обеспечения, которые вы выбираете вручную в списке. Этот список содержит все доступные обновления программного обеспечения.

  Например, вы можете задать обновления в следующих случаях: чтобы проверить установку обновлений в тестовом окружении, чтобы обновить только критически важные приложения или чтобы обновить только требуемые приложения.

- **Автоматически устанавливать все предыдущие обновления приложений, необходимые для установки выбранных обновлений**

  Включите этот параметр, если вы согласны с установкой промежуточных версий приложений, когда это необходимо, для установки выбранных обновлений.

  Если этот параметр выключен, устанавливаются только выбранные версии приложений. Выключите этот параметр, если вы хотите непосредственно обновить приложения, не пытаясь последовательно установить версии приложений. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

Например, у вас на устройстве установлена версия 3 приложения, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

По умолчанию параметр включен.

5. В окне **Уязвимости** выберите уязвимости, которые будут закрыты с установкой указанного обновления:

   - **Закрывать все уязвимости, соответствующие остальным критериям**

     В этом случае будут закрыты все уязвимости в приложениях, соответствующие критериям, указанным на шаге мастера **Общие критерии**. Выбрано по умолчанию.

   - **Закрыть только уязвимости из списка**

     Закрывать только уязвимости, которые выбраны вручную в списке. Этот список содержит все обнаруженные уязвимости.

     Например, вы можете задать уязвимости в следующих случаях: чтобы проверить закрытие уязвимостей в тестовом окружении, чтобы закрыть уязвимости только в критически важных приложениях или чтобы закрыть уязвимости только в требуемых приложениях.

6. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

Чтобы добавить правило для обновлений Центра обновления Windows:

1. Нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. На странице **Тип правила** выберите **Правило для обновлений Windows Update**.

3. В окне **Общие условия** настройте следующие параметры:

   - **Набор обновлений для установки**

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.

     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.

     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

- **Закрывать уязвимости с уровнем критичности по MSRC, равным или выше**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

  По умолчанию параметр выключен.

4. В окне **Приложения** выберите приложения и версии приложений, для которых вы хотите установить обновления. По умолчанию выбраны все приложения.

5. В окне **Категории обновлений** выберите категории обновлений для установки. Эти категории такие же, как и в каталоге Центра обновления Microsoft. По умолчанию выбраны все категории.

6. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

Чтобы добавить правило для обновления приложений сторонних производителей:

1. Нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. На странице **Тип правила** выберите **Правило для сторонних обновлений**.

3. В окне **Общие условия** настройте следующие параметры:

   - **Набор обновлений для установки**

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

     По умолчанию параметр выключен.

4. В окне **Приложения** выберите приложения и версии приложений, для которых вы хотите установить обновления. По умолчанию выбраны все приложения.

5. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе Параметры, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

Просмотр информации об уязвимостях в приложениях, обнаруженных на всех управляемых устройствах

После проверки программного обеспечения на управляемых устройствах на наличие уязвимостей вы можете просмотреть список обнаруженных уязвимостей в приложениях. Если вы запустите задачу для иерархии Серверов администрирования, вы можете просмотреть список управляемых устройств с обнаруженными уязвимостями только для выбранного Сервера администрирования.

Вы также можете сформировать и просмотреть отчет об уязвимостях.

Чтобы просмотреть список уязвимостей в приложениях, обнаруженных на всех управляемых устройствах,

В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

Отобразится список уязвимостей в приложениях, обнаруженных на клиентских устройствах.

Чтобы настроить список уязвимостей в приложениях,

Нажмите на значок **Фильтр** ( ) в верхнем правом углу списка уязвимостей в приложениях и выберите нужный фильтр. Вы также можете выбрать один из предустановленных фильтров в раскрывающемся списке **Предустановленные фильтры** над списком уязвимостей в приложениях.

Вы можете получить подробную информацию о любой уязвимости из списка.

Чтобы получить информацию об уязвимости в приложениях,

в списке уязвимостей в приложениях перейдите по ссылке с названием уязвимости.

Откроется окно свойств уязвимости в приложениях.

Просмотр информации об уязвимостях в приложениях, обнаруженных на выбранных управляемых устройствах

Вы можете просмотреть информацию об уязвимостях в приложениях, обнаруженных на выбранном управляемом устройстве под управлением Windows.

Чтобы просмотреть список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием устройства, для которого вы хотите просмотреть обнаруженные уязвимости в приложениях.

   Откроется окно свойств выбранного устройства.

3. В окне свойств выбранного устройства выберите вкладку **Дополнительно**.

4. На левой панели выберите раздел **Уязвимости в приложениях**.

Отобразится список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве.

Чтобы просмотреть свойства выбранной уязвимости в приложениях,

перейдите по ссылке с названием уязвимости в списке уязвимостей в приложениях.

Откроется окно свойств выбранной уязвимости в приложениях.

Просмотр статистики уязвимостей на управляемых устройствах.

Вы можете просмотреть статистическую информацию каждой уязвимости в приложениях на управляемых устройствах. Статистика представлена в виде диаграмм. На диаграмме отображается количество устройств со следующими статусами:

- *Игнорируется на: <количество устройств>*. Этот статус присваивается, если в свойствах уязвимости вы вручную установили параметр игнорировать уязвимость.
- *Закрыта на: <количество устройств>*. Этот статус присваивается, если задача закрытия уязвимости успешно завершена.
- *Запланирована к закрытию на: <количество устройств>*. Этот статус присваивается, если вы создали задачу закрытия уязвимостей, но задача пока еще не завершена.
- *Применено исправление на: <количество устройств>*. Этот статус присваивается, если вы вручную выбрали обновление программного обеспечения, чтобы закрыть уязвимость, но это обновление не закрыло уязвимость.
- *Требует закрытия на: <количество устройств>*. Этот статус присваивается, если уязвимость была закрыта только на некоторых управляемых устройствах, а уязвимость требуется закрыть на других управляемых устройствах.

Чтобы просмотреть статистику уязвимости на управляемых устройствах:

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

   Отобразится страница со списком уязвимостей в приложениях, обнаруженных на управляемых устройствах.

2. Установите флажок рядом с требуемой уязвимостью.

3. Нажмите на кнопку **Статистика уязвимостей на устройствах**.

   > Кнопка **Статистика уязвимостей на устройствах** недоступна, если вы выбрали более одной уязвимости.

   Отобразится диаграмма статусов уязвимости. Нажав на статус, откроется список устройств, на которых уязвимость имеет выбранный статус.

Экспорт списка уязвимостей в приложениях в текстовый файл

Вы можете скачать список отображаемых уязвимостей в файл формата CSV или TXT. Вы можете отправить эти файлы специалисту по безопасности или сохранить их для статистических целей.

Чтобы экспортировать список уязвимостей в приложениях, обнаруженных на всех управляемых устройствах, в текстовый файл:

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

Отображается список уязвимостей в приложениях, обнаруженных на управляемых устройствах.

По умолчанию экспортируются только уязвимости, отображаемые на текущей странице.

Если вы хотите экспортировать только определенные уязвимости, установите флажки рядом с этими уязвимостями.

2. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать. Если какая-либо из этих кнопок не отображается, нажмите на кнопку с многоточием и выберите нужный вариант в раскрывающемся списке.

На ваше устройство загружается файл со списком уязвимостей в приложениях.

Чтобы просмотреть список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве:

1. В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием устройства, для которого вы хотите просмотреть обнаруженные уязвимости в приложениях.

   Откроется окно свойств выбранного устройства.

3. В окне свойств выбранного устройства выберите вкладку **Дополнительно**.

4. На левой панели выберите раздел **Уязвимости в приложениях**.

Отобразится список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве.

По умолчанию экспортируются только уязвимости, отображаемые на текущей странице.

Если вы хотите экспортировать только определенные уязвимости, установите флажки рядом с этими уязвимостями.

1. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать. Если какая-либо из этих кнопок не отображается, нажмите на кнопку с многоточием и выберите нужный вариант в раскрывающемся списке.

На ваше устройство загружается файл со списком уязвимостей в приложениях.

Игнорирование уязвимостей в приложениях

Вы можете игнорировать уязвимости в приложениях и не закрывать их. Причины для игнорирования уязвимостей в приложениях могут быть, например, следующими:

- Вы не считаете, что уязвимость в приложении является критической для вашей организации.
- Вы понимаете, что закрытие уязвимости в приложениях может повредить данные приложения, для которого требуется закрыть уязвимость.
- Вы уверены, что уязвимость в приложениях не представляет опасности для сети вашей организации, так как вы используете другие меры для защиты управляемых устройств.

Вы можете игнорировать уязвимость в приложениях на всех управляемых устройствах или только на выбранных управляемых устройствах.

Чтобы пропустить уязвимость в приложениях на всех управляемых устройствах:

1. В главном окне приложения перейдите в раздел **Операции → Управление патчами → Уязвимости в приложениях**.

   Отображается список уязвимостей в приложениях, обнаруженных на управляемых устройствах.

2. В списке уязвимостей в приложениях нажмите на имя уязвимости в приложениях, которую вы хотите пропустить.

   Откроется окно свойств уязвимости в приложениях.

3. На вкладке **Общие** включите параметр **Игнорировать уязвимость**.

4. Нажмите на кнопку **Сохранить**.

   Окно свойств уязвимости в приложениях закроется.

Уязвимость в приложениях пропускается на всех управляемых устройствах.

Чтобы пропустить уязвимость в приложениях на выбранных управляемых устройствах:

1. В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с именем устройства, на котором вы хотите пропустить уязвимость в приложениях.

   Откроется окно свойств устройства.

3. В окне свойств устройства выберите раздел **Дополнительно**.

4. На левой панели выберите раздел **Уязвимости в приложениях**.

   Отобразится список уязвимостей в приложениях, обнаруженных на устройстве.

5. В списке уязвимостей в приложениях выберите уязвимость, которую вы хотите пропустить на выбранном устройстве.

   Откроется окно свойств уязвимости в приложениях.

6. В окне свойств уязвимости в приложениях на вкладке **Общие** включите параметр **Игнорировать уязвимость**.

7. Нажмите на кнопку **Сохранить**.

   Окно свойств уязвимости в приложениях закроется.

8. Закройте окно свойств устройства.

Уязвимость в приложениях пропускается на выбранном устройстве.

Пропущенные уязвимости в приложениях не будут закрыты после завершения работы задачи *Закрытие уязвимостей* и задачи *Установка требуемых обновлений и закрытие уязвимостей*. Вы можете исключить пропущенные уязвимости в приложениях из списка уязвимостей с помощью фильтра.

Сценарий: обнаружение и закрытие уязвимостей в приложениях

В этом разделе представлен сценарий обнаружения и закрытия уязвимостей на управляемых устройствах под управлением Windows. Вы можете обнаружить и закрыть уязвимости в операционной системе и в стороннем программном обеспечении, включая программное обеспечение Microsoft.

Предварительные требования

- Kaspersky SIEM Cloud развернут в вашей организации.
- В сети вашей организации есть управляемые устройства под управлением Windows.

Этапы

Обнаружение и закрытие уязвимостей состоит из следующих этапов:

1. **Поиск уязвимостей в программном обеспечении, установленном на клиентских устройствах**

   Чтобы найти уязвимости в приложениях, установленных на управляемых устройствах, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky SIEM Cloud получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, указанных в свойствах задачи и установленных на устройствах.

   Задача *Поиск уязвимостей и требуемых обновлений* автоматически создается в мастере первоначальной настройки Kaspersky SIEM Cloud. Если вы не запускали мастер первоначальной настройки, запустите его сейчас или создайте задачу вручную.

   Инструкции: Создание задачи Поиск уязвимостей и требуемых обновлений.

2. **Анализ списка обнаруженных уязвимостей в приложениях**

   Просмотрите список **Уязвимости в приложениях** и решите, какие уязвимости требуется закрыть. Чтобы просмотреть подробную информацию о каждой уязвимости, нажмите на имя уязвимости в списке. Для каждой уязвимости в списке вы также можете просмотреть статистику уязвимости на управляемых устройствах.

   Инструкции:

   - Просмотр информации об уязвимостях в приложениях.
   - Просмотр статистики уязвимостей на управляемых устройствах.

3. **Настройка закрытия уязвимостей**

   Обнаружив уязвимости в приложениях, вы можете закрыть уязвимости в приложениях на управляемых устройствах, используя задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Закрытие уязвимостей*.

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в приложениях сторонних производителей, в том числе в приложениях Microsoft, установленных на управляемых устройствах. Эта задача позволяет установить несколько обновлений и закрыть несколько уязвимостей в соответствии с определенными правилами. Доступность этой задачи зависит от режима Kaspersky Security Center Cloud Console и вашей действующей лицензии. Чтобы устранить уязвимости в приложениях, задача *Установка требуемых обновлений и закрытие уязвимостей* использует рекомендованные обновления приложений.

Задача *Закрытие уязвимостей* использует рекомендуемые исправления для программного обеспечения Microsoft.

Вы можете запустить мастер закрытия уязвимостей, который автоматически создаст одну из этих задач, или вы можете создать одну из этих задач вручную.

Инструкция: Закрытие уязвимостей в приложениях сторонних производителей, Создание задачи Установка требуемых обновлений и закрытие уязвимостей.

4. **Задание расписания задачи**

   Чтобы убедится, что список уязвимостей всегда актуален, задайте расписание запуска задачи *Поиск уязвимостей и требуемых обновлений*, чтобы она периодически запускалась автоматически. Рекомендуемый средний период – один раз в неделю.

   Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью, что и для задачи *Поиск уязвимостей и требуемых обновлений*, или реже. При задании расписания задачи *Закрытие уязвимостей*, вам нужно выбрать исправления приложений Microsoft каждый раз перед запуском задачи.

   При задании расписания задач убедитесь, что задача закрытия уязвимостей запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

5. **Игнорирование уязвимостей в приложениях (если требуется)**

   Вы можете игнорировать уязвимости в приложениях, которые должны быть закрыты на всех управляемых устройствах или только на выбранных управляемых устройствах.

   Инструкция: Игнорирование уязвимостей в приложениях

6. **Запуск задачи закрытия уязвимости**

   Запустите задачу *Установка требуемых обновлений и закрытие уязвимостей* или *Закрытие уязвимостей*. После завершения задачи убедитесь, что в списке задач она имеет статус *Завершена успешно*.

7. **Создание отчета о результатах закрытия уязвимостей в приложениях (если требуется)**

   Чтобы просмотреть статистику о закрытых уязвимостях, сформируйте отчет об уязвимостях. В отчете отображается информация об уязвимостях в приложениях, которые не закрыты. Таким образом, вы можете иметь представление об обнаружении и закрытии уязвимостей в приложениях сторонних производителей в вашей организации, включая программное обеспечение Microsoft.

   Инструкция: Создание и просмотр отчета.

8. **Проверка настройки обнаружения и закрытия уязвимостей в приложениях сторонних производителей**

   Убедитесь в следующем:

   - Список уязвимостей в приложениях на управляемых устройствах не пустой.
   - В списке задач есть задача закрытия уязвимостей.

- Запуск задач для поиска и закрытия уязвимостей в приложениях настроен так, чтобы они запускались последовательно. Просмотрите свойства этих задач и сравните их расписание.

- Задача закрытия уязвимостей в приложениях успешно выполнена. Просмотрите информацию в окне свойств задачи на вкладке **Результаты**.

Результаты

Если вы создали и настроили задачу *Установка требуемых обновлений и закрытие уязвимостей*, уязвимости будут автоматически закрыты на управляемых устройствах. При запуске задачи, задача выполняет сопоставление списка доступных обновлений программного обеспечения с правилами, указанными в параметрах задачи. Все обновления программного обеспечения, которые соответствуют критериям правил, будут загружены в хранилище точки распространения и будут установлены для закрытия уязвимостей в приложениях, кроме обновлений Центра обновления Windows. Для установки обновлений Windows вам необходимо обеспечить доступ к общедоступным серверам Центра обновления Windows на ваших управляемых устройствах.

Если вы создали задачу *Закрытие уязвимостей*, закрываются только уязвимости в приложениях Microsoft.

Установка максимального срока хранения информации о закрытых уязвимостях

Чтобы установить максимальный срок хранения в базе данных информации об уже закрытых уязвимостях на управляемых устройствах:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На открывшейся странице перейдите на вкладку **Хранилище событий**.

3. Укажите максимальный срок хранения информации о закрытых уязвимостях в базе данных.

   По умолчанию срок хранения составляет 7 дней в пробном режиме и 60 дней в коммерческом режиме. Максимальный срок хранения – 14 дней в пробном режиме и 365 дней в коммерческом режиме.

4. Нажмите на кнопку **Сохранить**.

Максимальный срок хранения информации о закрытых уязвимостях ограничен указанным количеством дней.

Управление запуском приложений на клиентских устройствах

В этом разделе описаны возможности Kaspersky SIEM Cloud связанные с управлением приложений, запущенных на клиентских устройствах.

Использование компонента Контроль приложений для управления исполняемыми файлами

Вы можете использовать компонент Контроль приложений, чтобы разрешить или запретить запуск исполняемых файлов на пользовательских устройствах. Компонент Контроль приложений поддерживает операционные системы Windows и Linux.

Для операционных систем Linux компонент Контроль приложений доступен, начиная с Kaspersky Endpoint Security 11.2 для Linux.

Предварительные требования

- Kaspersky SIEM Cloud развернут в вашей организации.
- Политика Kaspersky Endpoint Security for Windows или Kaspersky Endpoint Security for Linux создана и активна.

Этапы

Сценарий использования компонента Контроль приложений состоит из следующих этапов:

1. **Формирование и просмотр списка исполняемых файлов на клиентских устройствах**

   Этот этап помогает вам определить, какие исполняемые файлы обнаружены на управляемых устройствах. Просмотрите список исполняемых файлов и сравните его со списками разрешенных и запрещенных исполняемых файлов. Ограничения использования исполняемых файлов могут быть связаны с политиками информационной безопасности в вашей организации.

   Инструкция: Получение и просмотр списка исполняемых файлов, установленных на клиентских устройствах

2. **Создание категорий для исполняемых файлов, используемых в вашей организации**

   Проанализируйте списки исполняемых файлов, хранящихся на управляемых устройствах. На основе анализа сформируйте категории для исполняемых файлов. Рекомендуется создать категорию "Рабочие приложения", которая охватывает стандартный набор исполняемых файлов, используемых в вашей организации. Если разные группы безопасности используют свои наборы исполняемых файлов в своей работе, для каждой группы безопасности можно создать отдельную категорию.

   Инструкция: Создание пополняемой вручную категории приложений, Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств

3. **Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows**

   Настройте компонент Контроль приложений в политике Kaspersky Endpoint Security для Windows с использованием категорий, которые вы создали на предыдущем этапе.

   Инструкция: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows

4. **Включение компонента Контроль приложений в тестовом режиме**

   Чтобы правила Контроля приложений не блокировали исполняемые файлы, необходимые для работы пользователей, рекомендуется включить тестирование правил Контроля приложений и проанализировать их работу после создания правил. Когда тестирование включено, Kaspersky Endpoint Security для Windows не будет блокировать исполняемые файлы, запуск которых запрещен правилами Контроля приложений, а вместо этого будет отправлять уведомления об их запуске на Сервер администрирования.

   При тестировании правил Контроля приложений рекомендуется выполнить следующие действия:

   - Определите период тестирования. Период тестирования может варьироваться от нескольких дней до двух месяцев.
   - Изучите события, возникающие в результате тестирования работы компонента Контроль приложений.

   Инструкции: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows. Следуйте этой инструкции и включите тестовый режим в процессе настройки.

5. **Изменение параметров категорий компонента Контроль приложений**

   Если требуется, измените параметры компонента Контроль приложений. На основании результатов тестирования вы можете добавить исполняемые файлы, связанные с событиями компонента Контроль приложений, в категорию приложений пополняемую вручную.

   Инструкция: Добавление исполняемых файлов, связанных с событием, в категорию приложения.

6. **Применение правил Контроля приложений в рабочем режиме**

   После проверки правил Контроля приложений и завершения настройки категорий вы можете применить правила Контроль приложений в рабочем режиме.

   Инструкции: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows. Следуйте этой инструкции и выключите тестовый режим в процессе настройки.

7. **Проверка конфигурации Контроля приложений**

   Убедитесь в следующем:

   - Список категорий для исполняемых файлов не пуст. Просмотрите список категорий и убедитесь, что он содержит настроенные вами категории приложений.
   - Контроль приложений настроен на использование созданных категорий приложений. Просмотрите параметры политики Kaspersky Endpoint Security для Windows и убедитесь, что вы настроили Контроль приложений на вкладке **Параметры приложения** → **Контроль безопасности** → **Контроль приложений**.
   - Правила Контроля приложений применены в рабочем режиме. Проверьте режим в политике Kaspersky Endpoint Security для Windows и убедитесь, что вы выключили **Тестовый режим** на вкладке **Параметры приложения** → **Контроль безопасности** → **Контроль приложений**.

Результаты

После завершения сценария, запуск исполняемых файлов на управляемых устройствах контролируется. Пользователи могут запускать только те исполняемые файлы, которые разрешены в вашей организации, и не могут запускать исполняемые файлы, запрещенные в вашей организации.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security for Linux и Kaspersky Endpoint Security for Windows.

Режимы и категории компонента Контроль приложений

Компонент Контроль приложений контролирует попытки пользователей запуска приложений. Вы можете использовать правила компонента Контроль приложений для контроля запуска приложений.

Компонент Контроль приложений доступен для приложений Kaspersky Endpoint Security for Windows и Kaspersky Endpoint Security for Linux (версии 11.2 и выше). Все инструкции в этом разделе описывают настройку Контроля приложений для приложения Kaspersky Endpoint Security.

Запуск исполняемых файлов, параметры которых не соответствуют ни одному из правил Контроля приложений, регулируется выбранным режимом работы компонента:

- *Список запрещенных*. Режим используется, если вы хотите разрешить запуск всех исполняемых файлов, кроме тех, которые указаны в запрещающих правилах. По умолчанию выбран режим *Список запрещенных*.
- *Список разрешенных*. Режим используется, если вы хотите запретить запуск всех исполняемых файлов, кроме тех, которые указаны в разрешающих правилах.

Правила Контроля приложений реализованы в категориях для исполняемых файлов. В Kaspersky SIEM Cloud существует два типа категорий:

- Пополняемая вручную категория. Вы определяете условия, например, метаданные файла, хеш файла, сертификат файла, KL-категория, путь к файлу, чтобы включить исполняемые файлы в категорию.
- Категория, в которую входят исполняемые файлы с выбранных устройств. Вы указываете устройство, исполняемые файлы которого автоматически включаются в категорию.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security for Linux и Kaspersky Endpoint Security for Windows.

Получение и просмотр списка приложений, установленных на клиентских устройствах

Kaspersky SIEM Cloud выполняет инвентаризацию программного обеспечения, которое установлено на управляемых клиентских устройствах, работающих под управлением операционной системы Linux и Windows.

Агент администрирования составляет список приложений, установленных на устройстве, и передает список Серверу администрирования. Агенту администрирования требуется около 10–15 минут для обновления списка приложений.

Для клиентских устройств с операционной системой Windows Агент администрирования получает большую часть информации об установленных приложениях из реестра Windows. Для клиентских устройств с операционной системой Linux информацию об установленных приложениях Агент администрирования получает от диспетчеров пакетов.

Чтобы просмотреть список приложений, установленных на управляемых устройствах,

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Реестр приложений**.

   На странице отображается таблица с приложениями, установленными на управляемых устройствах. Выберите приложение, чтобы просмотреть свойства этого приложения, например: имя производителя, номер версии, список исполняемых файлов, список устройств, на которых установлено приложение, список доступных обновлений программного обеспечения или список обнаруженных уязвимостей программного обеспечения.

2. Вы можете группировать и фильтровать данные таблицы с установленными приложениями следующим образом:

   - Нажмите на значок параметров ( ) в правом верхнем углу таблицы.

     В открывшемся меню **Параметры таблицы** выберите столбцы, которые будут отображаться в таблице. Чтобы просмотреть тип операционной системы клиентских устройств, на которых установлено приложение, выберите столбец **Тип ОС**.

   - Нажмите на значок фильтрации ( ) в правом верхнем углу таблицы, укажите и примените критерий фильтрации в открывшемся меню.

     Отобразится отфильтрованная таблица установленных приложений.

Чтобы просмотреть список приложений, установленных на выбранном управляемом устройстве,

В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства → <имя устройства> → Дополнительно → Реестр приложений**. В этом меню можно экспортировать список приложений в файлы форматов CSV или TXT.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security for Linux и Kaspersky Endpoint Security for Windows.

Получение и просмотр списка исполняемых файлов, установленных на клиентских устройствах

Вы можете получить список исполняемых файлов, хранящихся на клиентских устройствах, одним из следующих способов:

- Включив уведомление о запуске приложений в политике Kaspersky Endpoint Security.
- Создав задачу инвентаризации.

Включение уведомлений о запуске приложений в политике Kaspersky Endpoint Security

Чтобы включить уведомления о запуске приложения:

1. Откройте параметры политики Kaspersky Endpoint Security и перейдите на вкладку **Общие параметры** → **Отчеты и хранилища**.
2. В группе параметров **Передача данных на Сервер администрирования** установите флажок **О запущенных приложениях** и сохраните изменения.

Когда пользователь пытается запустить исполняемые файлы, информация об этих файлах добавляется в список исполняемых файлов на клиентском устройстве. Kaspersky Endpoint Security отправляет эту информацию Агенту администрирования, а затем Агент администрирования отправляет ее на Сервер администрирования.

Создание задачи инвентаризации

Функция инвентаризации исполняемых файлов доступна для следующих приложений:

- Kaspersky Endpoint Security for Windows.
- Kaspersky Endpoint Security for Linux (версии 11.2 и выше).

Вы можете снизить нагрузку на базу данных при получении информации об установленных приложениях. Для этого рекомендуется запускать задачу инвентаризации на нескольких эталонных устройствах, на которых установлен стандартный набор приложений. Предпочтительное количество устройств равно 1–3.

Чтобы создать задачу инвентаризации исполняемых файлов на клиентских устройствах:

1. В главном окне приложения перейдите в раздел **Задачи**.

   Отобразится список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. На странице **Параметры новой задачи** в раскрывающемся списке **Приложение** выберите Kaspersky Endpoint Security for Windows или Kaspersky Endpoint Security for Linux в зависимости от типа операционной системы клиентских устройств.
4. В раскрывающемся списке **Тип задачи** выберите **Инвентаризация**.
5. На странице **Завершение создания задачи** нажмите на кнопку **Готово**.

После того как мастер создания задачи завершит свою работу, задача **Инвентаризация** будет создана и настроена. Вы можете изменить параметры созданной задачи. В результате созданная задача отобразится в списке задач.

Подробное описание задачи инвентаризации см. в следующих справках:

- Справка Kaspersky Endpoint Security for Windows
- Справка Kaspersky Endpoint Security for Linux

После выполнения задачи **Инвентаризация** формируется список исполняемых файлов, установленных на управляемых устройствах, и вы можете просмотреть этот список.

Во время инвентаризации могут быть обнаружены исполняемые файлы в следующих форматах (в зависимости от выбранного вами параметра в свойствах задачи инвентаризации): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR и HTML.

Просмотр списка приложений и исполняемых файлов, хранящихся на управляемых устройствах

Чтобы просмотреть список исполняемых файлов, хранящихся на клиентских устройствах,

В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Исполняемые файлы**.

На странице отобразится список исполняемых файлов, установленных на клиентских устройствах.

При необходимости вы можете отправить исполняемый файл управляемого устройства на устройство, где открыто приложение Open Single Management Platform.

Чтобы отправить исполняемый файл:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Исполняемые файлы**.
2. Перейдите по ссылке исполняемого файла, который вы хотите отправить.
3. В открывшемся окне перейдите в раздел **Устройства** и установите флажок рядом с управляемым устройством, с которого вы хотите отправить исполняемый файл.

   Перед отправкой исполняемого файла убедитесь, что управляемое устройство имеет прямое подключение к Серверу администрирования. Для этого вы можете использовать точку распространения в качестве push-сервера с портом по умолчанию (13295) или установить флажок **Не разрывать соединение с Сервером администрирования**. Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

4. Нажмите на кнопку **Отправить**.

Выбранный исполняемый файл будет загружен для дальнейшей отправки на устройство, на котором открыто приложение Open Single Management Platform.

Создание пополняемой вручную категории приложений

Вы можете указать набор критериев в качестве шаблона для исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов, соответствующих критериям, вы можете создать категорию приложений и использовать ее в настройке компонента Контроль приложений.

Чтобы создать пополняемую вручную категорию приложений:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Категории приложений**.

   Откроется страница со списком категорий приложений.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Выбор способа создания категории** выберите параметр **Пополняемая вручную категория. Данные об исполняемых файлах добавляются в категорию вручную**.

4. На шаге **Условия** нажмите на кнопку **Добавить**, чтобы добавить критерий условия для включения файлов в создаваемую категорию.

5. На шаге **Критерии условия** выполните следующие действия:

   a. Выберите тип правила для создания категории из списка:

   - **Из KL-категории**

     Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать категорию приложений "Лаборатории Касперского". Приложения, входящие в указанную KL-категорию, будут добавлены в пользовательскую категорию приложений.

   - **Выберите сертификат из хранилища сертификатов**

     Если выбран этот вариант, можно указать сертификаты из хранилища. Условие категории соответствует только исполняемым файлам, которые подписаны указанным сертификатом.

     Сертификаты будут добавлены в хранилище, если вы создали и запустили задачу инвентаризации или установили флажок **О запускаемых приложениях** в политике Kaspersky Endpoint Security. Вы можете выполнить оба действия.

     > Информация о сертификатах может быть извлечена только из исполняемых файлов формата PE (.exe, .dll, .sys).

   - **Задайте путь к приложению (поддерживаются маски)**

     Если выбран этот вариант, можно указать папку на клиентском устройстве, исполняемые файлы из которой будут добавлены в пользовательскую категорию приложений.

- **Съемный диск**

  Если выбран этот вариант, можно указать тип носителя (любой или съемный диск), на котором выполняется запуск приложения. Приложения, запускаемые на носителе выбранного типа, будут добавлены в пользовательскую категорию приложений.

- **Хеши файлов папки, метаданные файлов папки или сертификаты из папки**:

  - **Выберите из списка исполняемых файлов**

    Если выбран этот вариант, приложения для добавления в категорию можно выбрать из списка исполняемых файлов на клиентском устройстве.

  - **Выберите из реестра приложений**

    Если выбран этот параметр, отображается реестр приложений. После того как вы выберете приложение из реестра, откроется окно с параметрами, заполненными метаданными из выбранного вами приложения:

    - Имя файла.
    - Версия файла. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
    - Название приложения.
    - Версия приложения. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
    - Производитель.

    Обратите внимание, что блокируется только запуск исполняемых файлов, соответствующих указанным параметрам, но не запуск выбранного вами приложения. Если выбранные метаданные приложения совпадают с метаданными исполняемого файла, который запускается при запуске приложения, вы можете перейти к следующему шагу. Иначе вам нужно будет изменить значения вручную, чтобы они совпадали с метаданными исполняемого файла.

  - **Задайте вручную**

    Если выбран этот вариант, вам нужно указать хеш файла, метаданные или сертификат в качестве условия добавления приложений в пользовательскую категорию.

    Хеш файла

    В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky SIEM Cloud для файлов категории. Информация о хеш-значениях, вычисленных хеш-функциями, хранится в базе данных Сервера администрирования.

    SHA256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security для Linux поддерживает вычисление SHA256.

    Выберите один из вариантов вычисления хеш-функции приложением Kaspersky SIEM Cloud для файлов категории:

    - Если все экземпляры приложений безопасности, установленных в вашей сети, являются Kaspersky Endpoint Security for Linux, установите флажок **SHA256**.
    - Установите флажок **MD5-хеш**, только если вы используете Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux не поддерживает хеш-функцию MD5.

Метаданные

Если этот параметр выбран, вы можете указать метаданные файла такие как имя файла, версию файла и поставщика. Условие категории соответствует только исполняемым файлам с одинаковыми метаданными.

Сертификат

Если выбран этот вариант, можно указать сертификаты из хранилища. Условие категории соответствует только исполняемым файлам, которые подписаны указанным сертификатом.

Сертификаты будут добавлены в хранилище, если вы создали и запустили задачу инвентаризации или установили флажок **О запускаемых приложениях** в политике Kaspersky Endpoint Security. Вы можете выполнить оба действия.

- **Из файла MSI-пакета/архивной папки**

  Если выбран этот параметр, вы можете указать файл в архивной папке и выбрать, какое условие вы хотите использовать для добавления приложений в пользовательскую категорию. Архивная папка распаковывается, и выбранные условия применяются к файлам в этой папке. В качестве условия, можно выбрать один следующих критериев:

  - **Хеш файла**

    Вы можете выбрать, какую хеш-функцию (MD5 или SHA256) вы хотите использовать для вычисления значения хеш-функции. Приложения, имеющие такой же хеш, как и файлы в архивной папке, будут добавлены в пользовательскую категорию приложений.

    Выберите хеш-функцию MD5, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security for Linux не поддерживает хеш-функцию MD5.

  - **Метаданные**

    Выберите, какие метаданные вы хотите использовать в качестве критерия. Исполняемые файлы, имеющие такие же метаданные, будут добавлены в пользовательскую категорию приложений.

  - **Сертификат**

    Выберите, какие параметры сертификата (имя субъекта сертификата, отпечаток пальца или кем выписан сертификат) вы хотите использовать в качестве критерия. Исполняемые файлы, подписанные сертификатами, которые имеют те же параметры, будут добавлены в пользовательскую категорию.

  Для использования критериев **Метаданные** и **Сертификат** нужно вручную указать их после загрузки файла или архивной папки.

b. При необходимости добавьте комментарий в поле **Описание**. Количество символов не может превышать 1000.

   Позже вы можете изменить или удалить комментарий. Для этого в свойствах категории приложений откройте вкладку **Условия**, а затем в столбце **Критерий условия** перейдите по ссылке с условием, для которого вы хотите изменить или удалить комментарий.

   При выборе типа правила **Из KL-категории** вы можете добавить один комментарий для всех условий, которые будут созданы на основе этого типа правила. Вы можете изменить или удалить комментарий для каждого условия отдельно.

Выбранный критерий добавлен в список условий.

Вы можете добавить столько критериев для создания категории приложений, сколько вам нужно.

6. На шаге **Исключения** нажмите на кнопку **Добавить**, чтобы добавить критерий в область исключений и исключить файлы из создаваемой категории.

   При необходимости вы можете добавите комментарий в поле **Описание**. Количество символов не может превышать 1000.

   Позже вы можете изменить или удалить комментарий. Для этого в свойствах категории приложений откройте вкладку **Исключения**, а затем в столбце **Критерий условия** перейдите по ссылке с условием, для которого вы хотите изменить или удалить комментарий.

7. На шаге **Критерии условия**, выберите тип правила из списка, так же, как вы выбрали тип правила для создания категории.

После завершения мастера создается категория приложений. Оно появится в списке категорий приложений. Вы можете создать категорию приложений при настройке компонента Контроль приложений.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security for Linux и Kaspersky Endpoint Security for Windows.

Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств

Вы можете использовать исполняемые файлы с устройства как шаблон исполняемых файлов, запуск которых вы хотите разрешить или запретить. На основе исполняемых файлов с выбранных устройств вы можете создать категорию и использовать ее для настройки компонента Контроль приложений.

Чтобы создать категорию, в которую входят исполняемые файлы с выбранных устройств:

1. В главном окне приложения перейдите в раздел **Операции → Сторонние приложения → Категории приложений**.

   Откроется страница со списком категорий исполняемых файлов.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Выбор способа создания категории**, укажите имя категории и выберите параметр **Категория, в которую входят исполняемые файлы с выбранных устройств. Исполняемые файлы обрабатываются автоматически, их метрики заносятся в категорию**.

4. Нажмите на кнопку **Добавить**.

5. В открывшемся окне выберите устройство или устройства, чьи исполняемые файлы будут использоваться для создания категории.

6. Задайте следующие параметры:

   - **Алгоритм вычисления хеш-функции**

     В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением Kaspersky SIEM Cloud для файлов категории. Информация о хеш-значениях, вычисленных хеш-функциями, хранится в базе данных Сервера администрирования.

     SHA256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security для Linux поддерживает вычисление SHA256.

Выберите один из вариантов вычисления хеш-функции приложением Kaspersky SIEM Cloud для файлов категории:

- Если все экземпляры приложений безопасности, установленных в вашей сети, являются Kaspersky Endpoint Security for Linux, установите флажок **SHA256**.

- Установите флажок **MD5-хеш**, только если вы используете Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux не поддерживает хеш-функцию MD5.

По умолчанию флажок **Вычислять SHA256 для файлов в категории (поддерживается для версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** установлен.

По умолчанию флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)** снят.

- **Синхронизировать данные с хранилищем Сервера администрирования**

  Выберите этот параметр, если вы хотите, чтобы Сервер администрирования периодически выполнял проверку изменений в указанной папке (или папках).

  По умолчанию параметр выключен.

  Если вы включите этот параметр, укажите период (в часах), чтобы проверять изменения в указанной папке (папках). По умолчанию период проверки равен 24 часам.

- **Тип файла**

  В этом разделе вы можете указать тип файла, который используется для создания категории приложений.

  Все файлы. Для создаваемой категории учитываются все файлы. По умолчанию выбран этот вариант.

  Только файлы вне категорий приложений. Для создаваемой категории учитываются только файлы вне категорий приложений.

- **Папки**

  В этом разделе вы можете указать папки выбранных устройств, содержащие файлы, которые используются для создания категории приложений.

  Все папки. Для создаваемой категории учитываются все папки. По умолчанию выбран этот вариант.

  Указанная папка. Для создаваемой категории учитывается только указанная папка. Если вы выбирали этот параметр, вам нужно указать путь к папке.

По завершении работы мастера создается категория исполняемых файлов. Она появится в списке категорий. Вы можете создать категорию при настройке компонента Контроль приложений.

Просмотр списка категорий приложений

Вы можете просмотреть список настроенных категорий приложений и параметры каждой категории приложений.

Чтобы просмотреть список категорий приложений,

В главном окне приложения перейдите в раздел **Операции → Сторонние приложения → Категории приложений**.

Откроется страница со списком категорий приложений.

Чтобы просмотреть свойства категории приложений,

нажмите на имя категории приложений.

Откроется окно свойств выбранной категории приложений. Параметры сгруппированы на нескольких вкладках.

Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security for Windows

После создания категорий для Контроля приложений, вы можете использовать их для настройки Контроля приложений в политиках Kaspersky Endpoint Security for Windows.

Чтобы настроить компонент Контроль приложений в политике Kaspersky Endpoint Security for Windows:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

   Отобразится страница со списком политик.

2. Нажмите на политику **Kaspersky Endpoint Security for Windows**.

   Откроется окно свойств политики.

3. Перейдите в раздел **Параметры приложения** → **Контроль безопасности** → **Контроль приложений**.

   Отобразится окно **Контроль приложений** с параметрами компонента Контроль приложений.

4. Параметр **Контроль приложений** включен по умолчанию. Выключите переключатель **Контроль Программ [Выключен]**, чтобы выключить параметр.

5. В блоке **Параметры Контроля приложений** включите режим работы с применением правил Контроля приложений и разрешите Kaspersky Endpoint Security for Windows блокировку запуска приложений.

   Если вы хотите протестировать правила Контроля приложений, в разделе **Параметры Контроля приложений**, включите тестовый режим. В тестовом режиме Kaspersky Endpoint Security for Windows не блокирует запуск приложений, но фиксирует информацию о сработавших правилах в отчете. Перейдите по ссылке **Просмотреть отчет** для просмотра этой информации.

6. Включите параметр **Управление загрузкой модулей DLL**, если вы хотите, чтобы приложение Kaspersky Endpoint Security for Windows контролировало загрузку модулей DLL при запуске приложений пользователями.

   Информация о модуле и приложении, которое загрузило модуль, будет сохранена в отчете.

   Kaspersky Endpoint Security for Windows контролирует только DLL модули и драйверы, которые были загружены после того, как параметр **Управление загрузкой модулей DLL** был включен. Перезагрузите устройство после выбора параметра **Управление загрузкой модулей DLL**, если вы хотите, чтобы приложение Kaspersky Endpoint Security for Windows контролировало все модули и драйверы DLL, включая те, которые были загружены до запуска Kaspersky Endpoint Security for Windows.

7. (Если требуется.) В блоке **Шаблоны сообщений** измените шаблон сообщения, которое отображается, когда приложение заблокировано для запуска, и шаблон сообщения электронной почты, которое отправляется вам.

8. В блоке параметров **Режим Контроля приложений** выберите режим **Список запрещенных** или **Список разрешенных**.

   По умолчанию выбран режим **Список запрещенных**.

9. Перейдите по ссылке **Параметры списков правил**.

   Откроется окно **Списки запрещенных и разрешенных**, в котором можно добавить категорию приложений. По умолчанию отображается вкладка **Список запрещенных**, если выбран режим **Список запрещенных** или отображается вкладка **Список разрешенных**, если выбран режим **Список разрешенных**.

10. В окне **Списки запрещенных и разрешенных** нажмите на кнопку **Добавить**.

    Откроется окно **Правило Контроля приложений**.

11. Перейдите по ссылке **Пожалуйста, выберите категорию**.

    Откроется окно **Категории приложений**.

12. Добавьте категорию приложений (или категории), которые вы создали ранее.

    Вы можете изменить параметры категории, нажав на кнопку **Изменить**.

    Вы можете создать категорию, нажав на кнопку **Добавить**.

    Вы можете удалить категорию, нажав на кнопку **Удалить**.

13. После того как формирование списка категорий приложений завершено, нажмите на кнопку **ОК**.

    Окно **Категории приложений** закрывается.

14. В окне правил **Контроль приложений** в разделе **Субъекты и их права** создайте список пользователей и групп пользователей, чтобы применить к ним правила Контроля приложений.

15. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Правило Контроля приложений**.

16. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Списки запрещенных и разрешенных**.

17. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Контроль приложений**.

18. Закройте окно с параметрами политики Kaspersky Endpoint Security for Windows.

Компонент Контроль приложений настроен. После распространения политики на клиентские устройства запуск исполняемых файлов контролируется.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security for Linux и Kaspersky Endpoint Security for Windows.

Добавление исполняемых файлов, связанных с событием, в категорию приложения

После настройки компонента Контроль приложений в политиках Kaspersky Endpoint Security в списке событий могут отображаться следующие события:

- **Запуск приложения запрещен** (*Критическое* событие). Это событие отображается, если вы настроили Контроль приложений для применения правил.
- **Запуск приложения запрещен в тестовом режиме** (*Информационное* событие). Это событие отображается, если вы настроили Контроль приложений для применения правил в тестовом режиме.
- **Сообщение администратору о запрете запуска приложения** (сообщение с уровнем важности *Предупреждение*). Это событие отображается, если вы настроили Контроль приложений для применения правил, а пользователь запросил доступ к приложению, которое заблокировано для запуска.

Рекомендуется создавать выборки событий для просмотра событий, связанных с компонентом Контроль приложений.

Вы можете добавить исполняемые файлы, связанные с событиями Контроля приложений, в существующую категорию приложений или в новую категорию приложений. Вы можете добавлять исполняемые файлы только в категорию приложений пополняемую вручную.

Чтобы добавить исполняемые файлы, связанные с событиями компонента Контроль приложений, в категорию приложений:

1. В главном окне приложения перейдите в раздел **Мониторинг → Выборки событий**.

   Отобразится список выборок событий.

2. Выберите выборку событий, чтобы просмотреть события, связанные с Контролем приложений, и запустите формирование этой выборки событий.

   Если вы не создали выборку событий, связанную с Контролем приложений, вы можете выбрать и запустить предопределенную выборку, например, **Последние события**.

   Отобразится список событий.

3. Выберите события, связанные исполняемые файлы которых, вы хотите добавить в категорию приложений, и нажмите на кнопку **Назначить категорию**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. На странице мастера укажите необходимые параметры:

   - В разделе **Действие с исполняемым файлом, связанным с событием** выберите один из следующих вариантов:

     - **Добавить в новую категорию приложений**

       Выберите этот параметр, если вы хотите создать категорию приложений на основе исполняемых файлов, связанных с событиями.

       По умолчанию выбран этот вариант.

       Если вы выбрали этот параметр, укажите имя новой категории.

     - **Добавить в существующую категорию**

       Выберите этот параметр, если вы хотите добавить исполняемые файлы, связанные с событиями, в существующую категорию приложений.

       По умолчанию вариант не выбран.

Если вы выбрали этот параметр, выберите категорию приложений, пополняемую вручную, в которую вы хотите добавить исполняемые файлы.

- В разделе **Тип правила** выберите следующие параметры:
  - **Правила для добавления в область действия**
  - **Правила для добавления в исключения**
- В разделе **Параметр, используемый в качестве условия** выберите один из следующих вариантов:
  - **Данные сертификата (или SHA256 для файлов без сертификата)**

    Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одного приложения могут быть подписаны одним сертификатом или несколько разных приложений одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий приложения или несколько приложений одного производителя.

    Каждый файл имеет свою уникальную хеш-функцию SHA256. При выборе хеш-функции SHA256 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

    Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла или хеш-функцию SHA256 для файлов без сертификата.

    По умолчанию выбран этот вариант.

  - **Данные сертификата (файлы без сертификата пропускаются)**

    Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одного приложения могут быть подписаны одним сертификатом или несколько разных приложений одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий приложения или несколько приложений одного производителя.

    Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла. Если у исполняемого файла нет сертификата, то такой файл будет пропущен. Информация о нем не будет добавлена в категорию.

  - **Только SHA256 (файлы без хеша пропускаются)**

    Каждый файл имеет свою уникальную хеш-функцию SHA256. При выборе хеш-функции SHA256 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

    Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции SHA256 исполняемого файла.

  - **Только хеши MD5**

    Выберите этот параметр, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security for Linux не поддерживает хеш-функцию MD5.

    Каждый файл имеет свою уникальную хеш-функцию MD5. При выборе хеш-функции MD5 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

5. Нажмите на кнопку **OK**.

После завершения работы мастера исполняемые файлы, связанные с событиями Контроля приложений, добавляются в существующую категорию приложений или в новую категорию приложений. Вы можете

просмотреть параметры категории приложений, которую вы изменили или создали.

Подробное описание компонента Контроль приложений см. в онлайн-справке Kaspersky Endpoint Security for Linux и Kaspersky Endpoint Security for Windows.

Создание инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"

Kaspersky Security Center Web Console позволяет выполнять удаленную установку приложений сторонних производителей с помощью инсталляционных пакетов. Такие приложения сторонних производителей включены в соответствующую базу данных "Лаборатории Касперского".

Создание инсталляционных пакетов приложений сторонних производителя из базы "Лаборатории Касперского" доступно только при наличии лицензии на Системное администрирование.

Чтобы создать инсталляционный пакет для приложения стороннего производителя из базы "Лаборатории Касперского":

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Инсталляционные пакеты**.
2. Нажмите на кнопку **Добавить**.
3. На открывшейся странице мастера создания инсталляционного пакета выберите параметр **Выбрать приложение из базы "Лаборатории Касперского" для создания инсталляционного пакета** и нажмите на кнопку **Далее**.
4. В открывшемся списке приложений выберите соответствующее приложение и нажмите на кнопку **Далее**.
5. Выберите нужный язык локализации в раскрывающемся списке и нажмите на кнопку **Далее**.

   Этот шаг отображается только если приложение предоставляет несколько языков.

6. Если вам будет предложено принять Лицензионное соглашение для установки, на открывшейся странице **Лицензионное соглашение** перейдите по ссылке на веб-сайте производителя, чтобы прочитать Лицензионное соглашение, а затем установите флажок **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения настоящего Лицензионного соглашения**.
7. На открывшейся странице **Имя нового инсталляционного пакета** в поле **Имя пакета** укажите имя инсталляционного пакета и нажмите на кнопку **Далее**.

Дождитесь загрузки созданного инсталляционного пакета на Сервер администрирования. После того как мастер создания инсталляционного пакета отобразит сообщение, информирующее вас, что процесс создания пакета успешно завершен, нажмите на кнопку **Готово**.

Созданный инсталляционный пакет появится в списке инсталляционных пакетов. Вы можете выбрать этот пакет при создании или перенастройке задачи *Удаленная установка приложения*.

Просмотр и изменение параметров инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"

Если вы ранее создавали какие-либо инсталляционные пакеты приложений сторонних производителей, перечисленные в базе "Лаборатории Касперского", вы можете просмотреть и изменить параметры этих пакетов.

Изменение параметров инсталляционного пакета приложения стороннего производителя из базы "Лаборатории Касперского" доступно только при наличии лицензии на Системное администрирование.

Чтобы просмотреть и изменить параметры инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского":

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Инсталляционные пакеты**.
2. В открывшемся списке инсталляционных пакетов нажмите на имя соответствующего пакета.
3. На открывшейся странице свойств измените параметры, если это требуется.
4. Нажмите на кнопку **Сохранить**.

Изменения сохранены.

Параметры инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"

Параметры инсталляционного пакета приложения стороннего производителя сгруппированы на следующих вкладках:

Не все параметры, перечисленные ниже, отображаются по умолчанию. Вы можете добавить нужные столбцы, нажав на кнопку **Фильтр** и выбрав соответствующие имена столбцов из списка.

- Вкладка **Общие**:
  - Поле ввода, содержащее название инсталляционного пакета, которое можно изменить вручную.
  - **Приложение**

    Имя приложения стороннего производителя, для которого создан инсталляционный пакет.
  - **Версия**

    Номер версии приложения стороннего производителя, для которого создан инсталляционный пакет.

- **Размер**

  Размер инсталляционного пакета для приложения стороннего производителя (в килобайтах).

- **Создан**

  Дата и время создания инсталляционного пакета для приложения стороннего производителя.

- **Путь**

  Полный путь к сетевой папке, в которой находится инсталляционный пакет для приложения стороннего производителя.

- Вкладка **Последовательность установки**:

  - **Устанавливать требуемые общесистемные компоненты**

    Если флажок установлен, перед установкой обновления приложение автоматически устанавливает все общесистемные компоненты (пререквизиты), необходимые для установки этого обновления. Например, такими пререквизитами могут являться обновления операционной системы.

    Если этот параметр выключен, необходимо установить пререквизиты вручную.

    По умолчанию параметр выключен.

  - Таблица, в которой отображаются свойства обновления и которая содержит следующие графы:

    - **Имя**

      Название обновления.

    - **Описание**

      Описание обновления.

    - **Источник**

      Источник обновления, то есть выпущено ли обновление Microsoft или другим сторонним производителем.

    - **Тип**

      Тип обновления, то есть предназначено ли обновление для драйвера или приложения.

    - **Категория**

      Категория служб Windows Server Update Services (WSUS), отображаемая для обновлений Microsoft (Критические обновления, Обновления определений, Драйверы, Пакеты дополнительных компонентов, Обновления системы безопасности, Пакеты обновления, Средства, Накопительные пакеты обновления, Обновления или Обновления с предыдущих версий).

    - **Уровень важности по MSRC**

      Уровень важности обновления, определенный Microsoft Security Response Center (MSRC).

    - **Уровень важности**

      Уровень важности обновления определен "Лабораторией Касперского".

- **Уровень важности патча**

  Уровень важности патча, если он предназначен для приложений "Лаборатории Касперского".

- **Статья**

  Идентификатор статьи в Базе знаний с описанием обновления.

- **Бюллетень**

  Идентификатор бюллетеня безопасности с описанием обновления.

- **Не назначено к установке (новая версия)**

  Отображается, имеет ли обновление статус Не назначено к установке.

- **Назначено к установке**

  Отображается, имеет ли обновление статус Назначено к установке.

- **Устанавливается**

  Отображается, имеет ли обновление статус Устанавливается.

- **Установлено**

  Отображается, имеет ли обновление состояние Установлено.

- **Сбой**

  Отображается, имеет ли обновление статус Сбой.

- **Требуется перезагрузка**

  Отображается, имеет ли обновление статус Требуется перезагрузка.

- **Зарегистрировано**

  Отображается дата и время, когда обновление было зарегистрировано.

- **Устанавливается интерактивно**

  Отображается, требуется ли взаимодействие с пользователем во время установки обновления.

- **Статус одобрения обновления**

  Отображается, одобрена ли установка обновления.

- **Ревизия**

  Отображается номер текущей ревизии обновления.

- **Идентификатор обновления**

  Отображается идентификатор обновления.

- **Версия приложения**

  Отображается номер версии, до которой должно быть обновлено приложение.

- **Заменяемое**

  Отображаются другие обновления, которые могут заменить это обновление.

- **Заменяющее**

  Отображаются другие обновления, которые можно заменить этим обновлением.

- **Требуется принять условия Лицензионного соглашения**

  Отображается, требует ли обновление согласие с условиями Лицензионного соглашения.

- **Описание веб-адреса**

  Отображается имя поставщика обновлений.

- **Семейство приложений**

  Отображается имя семейства приложений, к которым относится обновление.

- **Приложение**

  Отображается название приложения, которому принадлежит обновление.

- **Язык локализации**

  Отображается язык локализации обновления.

- **Не назначено к установке (новая версия)**

  Отображается, имеет ли обновление статус Не назначено к установке (новая версия).

- **Требует установки пререквизитов**

  Отображается, имеет ли обновление состояние Требует установки пререквизитов.

- **Режим загрузки**

  Отображается режим загрузки обновлений.

- **Является патчем**

  Отображается, является ли обновление патчем.

- **Не установлено**

  Отображается, имеет ли обновление статус Не установлено.

- **Создан**

- Вкладка **Параметры**, на которой отображаются параметры инсталляционного пакета, их названия, описания и значения, которые используются в качестве параметров командной строки во время установки. Если в пакете таких нет параметров, отображается соответствующее сообщение. Вы можете изменить значения этих параметров.

- Вкладка **История ревизий**, на которой отображается версии инсталляционного пакета и которая содержит следующие графы:
  - **Ревизия** – номер версии инсталляционного пакета.
  - **Время** – дата и время изменения параметров инсталляционного пакета.
  - **Пользователь** – имя пользователя, изменившего параметры инсталляционного пакета.
  - **IP-адрес устройства пользователя** – IP-адрес устройства, с которого был изменен объект.
  - **IP-адрес Web Console** – IP-адрес приложения OSMP Console, с помощью которого был изменен объект.
  - **Действие** – действия, которые были выполнены с инсталляционным пакетом в этой ревизии.
  - **Описание** – описание ревизии изменения параметров инсталляционного пакета.

    По умолчанию описание ревизии не заполнено. Чтобы добавить описание ревизии, выберите нужную ревизию и нажмите на кнопку **Изменить описание**. В открывшемся окне введите текст описания ревизии.

Теги приложений

Kaspersky SIEM Cloud позволяет назначать теги приложениям из реестра приложений. Тег представляет собой метку приложения, которую можно использовать для группировки и поиска приложений. Назначенный приложению тег можно использовать в условиях для выборок устройств.

Например, можно создать тег `[Browsers]` и назначить его всем браузерам, таким как Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

Создание тегов приложений

Чтобы создать тег приложения:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением → Сторонние приложения → Теги приложений**.
2. Нажмите на кнопку **Добавить**.

   Отобразится окно создания тега.
3. Укажите тег.
4. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Новый созданный тег появляется в списке тегов приложения.

Изменение тегов приложений

Чтобы переименовать тег приложения:

1. В главном окне приложения перейдите в раздел **Операции** → **Сторонние приложения** → **Теги приложений**.
2. Установите флажок рядом с тегом, который вы хотите переименовать, и нажмите на кнопку **Изменить**.

   Откроется окно свойств тега.
3. Измените имя тега.
4. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Обновленный тег появится в списке тегов приложений.

Назначение тегов приложениям

Чтобы назначить приложению теги:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Сторонние приложения** → **Реестр приложений**.
2. Выберите приложение, для которого требуется назначить теги.
3. Выберите вкладку **Теги**.

   На вкладке появятся все теги приложений, существующие на Сервере администрирования. Теги, назначенные выбранному приложению, отмечены флажками в столбце **Назначенный тег**.
4. Установите флажки в столбце **Назначенный тег** для тегов, которые требуется назначить.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Теги назначены приложению.

Снятие назначенных тегов с приложений

Чтобы снять теги с приложения:

1. В главном окне приложения перейдите в раздел **Управление программным обеспечением** → **Сторонние приложения** → **Реестр приложений**.
2. Выберите приложение, с которого требуется снять теги.
3. Выберите вкладку **Теги**.

   На вкладке появятся все теги приложений, существующие на Сервере администрирования. Теги, назначенные выбранному приложению, отмечены флажками в столбце **Назначенный тег**.

4. Снимите флажки в столбце **Назначенный тег** для тегов, которые требуется снять.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Теги будут сняты с приложения.

Снятые с приложений теги не удаляются. При необходимости их можно удалить вручную.

Удаление тегов приложений

Чтобы удалить тег приложения:

1. В главном окне приложения перейдите в раздел **Операции** → **Сторонние приложения** → **Теги приложений**.

2. В списке выберите теги приложения, которые вы хотите удалить.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **ОК**.

Выбранный тег приложения удален. Удаленный тег автоматически снимается со всех приложений, которым он был назначен.

Настройка Сервера администрирования

В этом разделе описан процесс настройки и свойства Сервера администрирования.

Иерархия Серверов администрирования

Некоторые компании-клиенты, например MSP-клиенты, могут использовать несколько Серверов администрирования. Администрировать несколько разрозненных Серверов неудобно, поэтому целесообразно объединять их в иерархию. Для Сервера администрирования, который находится в инфраструктуре "Лаборатории Касперского", и главный, и подчиненный Серверы администрирования в вашей сети являются подчиненными. Вы можете добавить как Сервер администрирования с системой Windows, так и Сервер администрирования с системой Linux.

Взаимодействие "главный – подчиненный" между двумя Серверами администрирования предоставляет следующие возможности:

- Подчиненный Сервер наследует с главного Сервера политики, задачи, роли пользователей и инсталляционные пакеты, устраняется дублирование параметров.

- Выборки устройств на главном Сервере могут включать в себя устройства с подчиненных Серверов.

- Отчеты на главном Сервере могут включать в себя данные (в том числе и детальные) с подчиненных Серверов.

- Главный Сервер администрирования может использоваться в качестве источника обновлений для подчиненного Сервера администрирования.

Главный Сервер администрирования, установленный в основной инфраструктуре организации, выполняет в роль главного тенанта. Главный Сервер администрирования позволяет подчиненным или виртуальным Серверам администрирования (и его изолированным тенантам) независимо получать и обрабатывать свои события, а также работать со своими ресурсами, службами и конфигурациями.

Поставщик услуг, у которого есть несколько организаций-клиентов, может предоставить функциональность Open Single Management Platform, включая агрегирование алертов и действия по реагированию, каждой организации-клиенту независимо. Для этого поставщик услуг подключает подчиненные или виртуальные Серверы администрирования в качестве тенантов для каждой организации-клиента. Поставщик услуг предоставляет услуги, используя свой собственный персонал и ресурсы.

Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования

Вы можете назначить Сервер администрирования, работающий локально, подчиненным Сервером, установив таким образом отношение иерархии "главный Сервер – подчиненный Сервер" внутри вашей сети. Для Сервера администрирования, который находится в инфраструктуре "Лаборатории Касперского", и главный, и подчиненный Серверы администрирования в вашей сети являются подчиненными. Вы можете добавить как Сервер администрирования с системой Windows, так и Сервер администрирования с системой Linux.

Чтобы добавить подчиненный Сервер администрирования, доступный для подключения:

1. Убедитесь, что на будущем подчиненном Сервере администрирования установлено приложение Kaspersky Security Center Web Console.

2. На будущем подчиненном Сервер администрирования загрузите сертификат Сервера администрирования и сохраните его, чтобы его можно было добавить на главный Сервер администрирования на одном из шагов мастера добавления подчиненного Сервера администрирования.

3. Выполните следующие действия через Kaspersky Security Center Web Console на будущем подчиненном Сервере администрирования (также вы можете предложить выполнить эти действия администратору будущего подчиненного Сервера администрирования):

   a. Перейдите в свойства будущего главного Сервера администрирования, нажав на название Сервера администрирования в главном меню.

      Вы также можете перейти к свойствам нужного Сервера администрирования из панели навигации. Для этого в главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Settings**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**. В открывшейся панели наведите курсор мыши на название нужного Сервера администрирования и нажмите на значок параметров (⚙).

   b. В открывшемся окне свойств перейдите в раздел **Иерархия Серверов администрирования** на вкладку **Общие**.

   c. Выберите параметр **Этот Сервер администрирования является подчиненным в иерархии**.

d. Выберите тип **Cloud Console** в качестве типа главного Сервера администрирования.

Поля становятся доступными для установки соединения между подчиненным и главным Серверами администрирования.

e. В полях **Адрес HDS-сервера (для главного Сервера администрирования на Kaspersky Security Center Cloud Console)** и **Порты HDS-сервера** укажите адрес и порт главного Сервера администрирования Kaspersky Security Center Cloud Console.

Вы можете найти адрес HDS-сервера и порт HDS-сервера в интерфейсе Kaspersky Security Center Cloud Console Administration Server в разделе **Иерархия Серверов администрирования** на вкладке **Общие** окна свойств. Вы можете скопировать и вставить эти данные в поля окна свойств подчиненного Сервера администрирования.

f. Нажмите на кнопку **Укажите сертификат главного Сервера администрирования** и выберите сертификат.

Вы можете загрузить этот сертификат с Сервера администрирования Kaspersky Security Center Cloud Console в разделе **Иерархия Серверов администрирования** на вкладке **Общие** окна свойств, нажав на кнопку **Посмотреть сертификат Сервера**.

g. Нажмите на кнопку **Укажите сертификат службы Hosted Discovery Service** и выберите сертификат.

Вы можете загрузить этот сертификат с Сервера администрирования Kaspersky Security Center Cloud Console в разделе **Иерархия Серверов администрирования** на вкладке **Общие** в окне свойств, нажав на кнопку **HDS-сертификат, выпущенный корневым центром сертификации**.

h. Если вы используете прокси-сервер для подключения к Серверу администрирования Kaspersky Security Center Cloud Console (то есть к главному Серверу в построенной вами иерархии), укажите это и введите учетные данные прокси-сервера.

i. Выберите параметр **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**, если подчиненный Сервер администрирования находится в демилитаризованной зоне (DMZ).

j. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения и закрыть окно.

4. В главном меню Kaspersky Security Center Cloud Console нажмите на имя Сервера администрирования.

5. На открывшейся странице свойств нажмите на вкладку **Серверы администрирования**.

6. Установите флажок рядом с именем группы администрирования, в которую вы хотите добавить подчиненный Сервер администрирования.

7. В меню выберите пункт **Подключить подчиненный Сервер администрирования**.

Запустится мастер добавления подчиненного Сервера администрирования. Для продолжения работы мастера нажмите на кнопку **Далее**.

8. Заполните следующие поля:

- **Имя подчиненного Сервера администрирования**

  Имя подчиненного Сервера администрирования, которое будет отображаться в иерархии Серверов. Вы можете ввести IP-адрес в качестве имени или использовать такое имя, как, например, "Подчиненный Сервер для группы 1".

- **Адрес подчиненного Сервера администрирования (необязательно)**

  Укажите IP-адрес или доменное имя подчиненного Сервера администрирования.

Этот параметр необходим, если включен параметр **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.

9. Если вы используете прокси-сервер для подключения к Серверу администрирования Kaspersky Security Center Cloud Console (то есть будущему главному Серверу), укажите это и введите учетные данные прокси-сервера.

10. Следуйте далее указаниям мастера.

После завершения работы мастера иерархия "главный Сервер – подчиненный Сервер" создана. Главный Сервер начинает принимать подключение от подчиненного Сервера через порт 13000. Задачи и политики главного Сервера администрирования получены и применены. Подчиненный Сервер администрирования отображается на главном Сервере администрирования, в группе администрирования, в которую он был добавлен.

Настройка срока хранения событий, относящихся к удаленным устройствам

В Kaspersky Security Center Cloud Console события хранятся в хранилище событий. Вы не можете настраивать количество событий, которые хранятся в хранилище событий.

В окне свойств Сервера администрирования, в разделе **Хранилище событий** вы можете настроить максимальный срок хранения событий, относящихся к удаленным устройствам. Максимальный срок хранения – 1000 дней.

Чтобы настроить количество дней хранения событий, относящихся к удаленным устройствам:

1. В главном окне приложения нажмите на имя Сервера администрирования.

Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Хранилище событий**.

3. Включите параметр **Хранить события после удаления устройств**.

4. В блоке **Максимальное время хранения (сут)** укажите количество дней хранения событий, относящихся к удаленным устройствам.

Количество дней хранения событий, относящихся к удаленным устройствам, ограничено указанным значением.

Также можно изменить параметры любой задачи, чтобы сохранять события, связанные с ходом выполнения задачи, или сохранять только результаты выполнения задачи. Таким образом вы уменьшаете количество событий в базе данных, увеличиваете скорость работы сценариев, связанных с анализом таблицы событий в базе данных, и снижаете риск вытеснения критических событий большим количеством событий.

Объединение электронной почты о событиях

Во время работы Kaspersky Security Center Cloud Console и управляемые приложения "Лаборатории Касперского" генерируют события. Каждое событие относится к определенному типу и уровню важности (*Критическое событие*, *Отказ функционирования*, *Предупреждение*, *Информационное сообщение*). В зависимости от условий, при которых произошло событие, приложение Kaspersky Security Center Cloud Console может присваивать событиям одного типа разные уровни важности.

Kaspersky Security Center Cloud Console автоматически отправляет уведомления о событиях по электронной почте. Kaspersky Security Center Cloud Console отправляет уведомления о событиях, перечисленных в окне **Свойства Сервера администрирования** на вкладке **Настройка событий**. Общие параметры уведомлений используются для всех типов событий.

Чтобы ограничить количество отправляемых электронных писем, Kaspersky Security Center Cloud Console объединяет события с одинаковым уровнем важности за указанные периоды. Значения периодов управляются специалистами "Лаборатории Касперского". При необходимости вы можете просмотреть информацию об интервалах объединения, **перейдя по этой ссылке**.

После отправки уведомления о новом событии с определенным уровнем важности Сервер администрирования выполняет следующие действия:

1. Активирует пятнадцатиминутный счетчик.

2. Через 15 минут:

   - Если не произошло ни одного события такого же или более низкого уровня важности, счетчик сбрасывается.

   - Если происходит хотя бы одно событие с таким же или более низким уровнем важности, отправляет получателям одно объединенное письмо с информацией о событиях, а затем активирует другой счетчик с трехчасовым интервалом.

     В этом случае Сервер администрирования выполняет одно из следующих действий:

     - Если в течение этих трех часов не произошло ни одного события соответствующего (или более низкого) уровня важности, оба счетчика сбрасываются.

     - Если происходит хотя бы одно событие с таким же или более низким уровнем важности, отправляет получателям одно объединенное электронное письмо с информацией о событиях и повторно активирует трехчасовой счетчик.

Если в течение одного из интервалов (15 минут или 3 часов) происходит хотя бы одно событие с более высоким уровнем важности, Сервер администрирования последовательно выполняет следующие действия:

a. Отправляет получателям одно объединенное письмо с информацией о ранее накопленных событиях, не дожидаясь окончания интервала.

b. Отправляет получателям электронное сообщение о новом событии с более высоким уровнем важности.

c. Сбрасывает активные счетчики.

d. Активирует новый 15-минутный счетчик и описанный здесь сценарий будет перезапущен.

В результате получателям приходят объединенные электронные письма в соответствии со следующим шаблоном: "Произошли события: <Количество> <Уровень_важности> (и более низкого уровня)".

Если вы хотите получать уведомления от пользователей немедленно, вы можете настроить интеграцию между Kaspersky Security Center Cloud Console и SIEM, а затем настроить уведомления о необходимых событиях из SIEM.

Ограничения на управление подчиненными Серверами администрирования, работающими локально, с помощью Kaspersky Security Center Cloud Console

После перехода на подчиненный Сервер администрирования, работающий локально, с помощью соответствующего параметра в Kaspersky Security Center Cloud Console, приложение накладывает определенные ограничения на управление этим подчиненным Сервером администрирования. Следующие параметры, относящиеся к работе Kaspersky Next XDR Expert, становятся недоступными для пользователя:

- В свойствах политик Агента администрирования и политик Сервера администрирования вкладки **Настройка событий** и **Параметры приложения** недоступны; невозможно создать политики.
- В свойствах задач Агента администрирования и задач Сервера администрирования вкладки **Настройка событий** и **Параметры приложения** недоступны; невозможно создать задачи.
- Управление Агентом администрирования и Сервером администрирования недоступно, также недоступно окно свойств подчиненного Сервера администрирования.
- Мастер первоначальной настройки недоступен.
- Параметры хранения событий и уведомлений для Агента администрирования и Сервера администрирования не могут быть изменены.
- Раздел **Каталог приложений "Лаборатории Касперского"** недоступен.
- Раздел **Инсталляционные пакеты** недоступен.

Просмотр списка подчиненных Серверов администрирования

Чтобы просмотреть список подчиненных (включая виртуальные) Серверов администрирования:

1. В главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**).
2. В верхней части страницы нажмите на кнопку **Показать иерархию**.

   В открывшейся панели навигации отобразится список подчиненных (в том числе виртуальных) Серверов администрирования. Вы можете перейти на любой из этих Серверов администрирования, нажав на его имя.

Вы не сможете перейти к виртуальным Серверам администрирования, если вы открыли панель навигации из разделов **IP-диапазоны** и **Удаленные объекты**.
Также отображаются группы администрирования. Группы доступны для управления, если вы открыли панель навигации из следующих разделов: **Управляемые устройства**, **Политики**, **Задачи** и **Точки распространения**. Иначе группы отображаются серым цветом.

Удаление иерархии Серверов администрирования

Если вам больше не нужна иерархия Серверов администрирования, вы можете отключить их от этой иерархии.

Чтобы удалить иерархию Серверов администрирования:

1. В главном меню нажмите на имя главного Сервера администрирования.
2. На открывшейся странице перейдите на вкладку **Серверы администрирования**.
3. В группе администрирования, в которой вы хотите удалить подчиненный Сервер администрирования, выберите подчиненный Сервер администрирования.
4. В меню выберите пункт **Удалить**.
5. В открывшемся окне нажмите на кнопку **ОК** для подтверждения удаления подчиненного Сервера администрирования.

   Бывший главный и бывшие подчиненные Серверы администрирования теперь независимы друг от друга. Иерархии Серверов больше не существует.

Настройка интерфейса

Вы можете настроить интерфейс OSMP Console, чтобы отобразить или скрыть разделы и элементы интерфейса в зависимости от используемых функций.

Чтобы настроить интерфейс OSMP Console в соответствии в соответствии с используемым в настоящее время набором функций:

1. В главном окне приложения перейдите в раздел **Параметры** → **Параметры интерфейса**.
2. В появившемся окне **Параметры интерфейса** включите или выключите параметры:
   - **Показать раздел "Шифрование и защита данных"**

     Вы можете использовать этот параметр, чтобы скрыть или отобразить раздел **Операции** → **Шифрование и защита данных** в интерфейсе. OSMP Console сохраняет значение этого параметра только для вашей учетной записи; при этом другой пользователь может установить другое значение.
   - **Показать функции MDR**

     Вы можете использовать этот параметр, чтобы скрыть или отобразить раздел **Мониторинг** → **Инциденты** в интерфейсе. OSMP Console сохраняет значение этого параметра только для вашей учетной записи; при этом другой пользователь может установить другое значение.
3. Укажите количество устройств, которое OSMP Console будет отображать в результатах распространения политики.
4. Нажмите на кнопку **Сохранить**.

Параметры интерфейса настроены в соответствии с вашими требованиями.

Управление виртуальными Серверами администрирования

В этом разделе описываются следующие действия, как управлять виртуальными Серверами администрирования:

- создание виртуальных Серверов администрирования;
- включение и выключение виртуальных Серверов администрирования;
- назначение администратора виртуального Сервера администрирования;
- смена Сервера администрирования для клиентских устройств;
- удаление виртуальных Серверов администрирования.

Создание виртуального Сервера администрирования

Можно создать виртуальные Серверы администрирования и добавить их в группы администрирования.

Чтобы создать и добавить виртуальный Сервер администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.
2. На открывшейся странице выберите вкладку **Серверы администрирования**.

3. Выберите группу администрирования, в которую вы хотите добавить виртуальный Сервер администрирования.

4. В меню выберите пункт **Новый виртуальный Сервер администрирования**.

5. На открывшейся странице укажите **Имя виртуального Сервера администрирования**.

6. Нажмите на кнопку **Сохранить**.

Новый виртуальный Сервер администрирования создан, добавлен в группу администрирования и отображается на вкладке **Серверы администрирования**.

Включение и выключение виртуального Сервера администрирования

Когда вы создаете виртуальный Сервер администрирования, он по умолчанию включается. Вы можете выключить или снова включить его в любое время. Выключение или включение виртуального Сервера администрирования равносильно выключению или включению физического Сервера администрирования.

Чтобы включить или выключить виртуальный Сервер администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.

2. На открывшейся странице перейдите на вкладку **Серверы администрирования**.

3. Выберите виртуальный Сервер администрирования, который вы хотите включить или выключить.

4. В меню нажмите на кнопку **Подключить / отключить виртуальный Сервер администрирования**.

Состояние виртуального Сервера администрирования изменяется на включено или выключено в зависимости от его предыдущего состояния. Обновленное состояние отображается рядом с именем Сервера администрирования.

Назначение администратора виртуального Сервера администрирования

Если вы используете в своей организации виртуальные Серверы администрирования, вам может потребоваться назначить отдельного администратора для каждого виртуального Сервера администрирования. Например, это может быть полезно, когда вы создаете виртуальные Серверы администрирования для управления отдельными офисами или отделами вашей организации или если вы являетесь поставщиком услуг (MSP) и управляете своими тенантами с помощью виртуальных Серверов администрирования.

При создании виртуального Сервера администрирования он наследует список пользователей и все права пользователей главного Сервера администрирования. Если пользователь имеет права доступа к главному Серверу, этот пользователь также имеет права доступа к виртуальному Серверу. После создания вы самостоятельно настраиваете права доступа к Серверам. Если вы хотите назначить администратора только для виртуального Сервера администрирования, убедитесь, что администратор не включен в список **Права доступа** в свойствах главного Сервера администрирования.

Вы назначаете администратора виртуального Сервера администрирования, предоставляя права доступа администратору к виртуальному Серверу администрирования. Вы можете предоставить требуемые права доступа одним из следующих способов:

- Настройте права доступа для администратора вручную.
- Назначьте одну или несколько пользовательских ролей администратору.

При назначении администратора убедитесь, что вы предоставляете доступ к одному виртуальному Серверу администрирования. Администратор, имеющий доступ к нескольким виртуальным Серверам администрирования, не может войти в Kaspersky Security Center Cloud Console.

Администратор виртуального Сервера администрирования входит в Kaspersky Security Center Cloud Console так же, как и на главный Сервер администрирования. Kaspersky Security Center Cloud Console выполняет аутентификацию администратора и открывает виртуальный Сервер администрирования, к которому у администратора есть права доступа. Администратор не может переключаться между Серверами администрирования.

Предварительные требования

Убедитесь, что выполнены следующие условия:

- Виртуальный Сервер администрирования создан.
- На главном Сервере администрирования у вас создана учетная запись для администратора, которого вы хотите назначить для виртуального Сервера администрирования.
- Созданная учетная запись администратора виртуального Сервера не включается в список **Права доступа** в свойствах любых Серверов, главных и подчиненных.
- У вас есть право **Изменение списков управления доступом объектов** в функциональной области **Общие функции** → **Права пользователей**.

Настройка прав доступа вручную

Чтобы назначить администратора виртуального Сервера администрирования:

1. Переключитесь на нужный виртуальный Сервер администрирования:
   a. В главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**.
   b. В открывшейся панели нажмите на имя нужного виртуального Сервера администрирования.

   Вы не можете переключиться на виртуальный Сервер администрирования из разделов **IP-диапазоны** и **Удаленные объекты**.

   В главном меню Сервер администрирования изменится на тот, который вы выбрали.

2. Перейдите в свойства Сервера администрирования, нажав на его имя в главном меню.

   Или в панели наведите курсор мыши на название нужного виртуального Сервера администрирования и нажмите на значок параметров (⚙).

   Откроется окно свойств Сервера администрирования.

3. На вкладке **Права доступа** нажмите на кнопку **Добавить**.

   Откроется единый список пользователей главного Сервера администрирования и текущего виртуального Сервера администрирования.

4. В списке пользователей выберите учетную запись администратора, которого вы хотите назначить для виртуального Сервера администрирования, и нажмите на кнопку **ОК**.

   Приложение добавляет выбранного пользователя в список пользователей на вкладку **Права доступа**.

5. Установите флажок рядом с добавленной учетной записью и нажмите на кнопку **Права доступа**.

6. Настройте права администратора на виртуальном Сервере администрирования.

   Для успешной аутентификации администратор должен иметь следующие права:

   - право **Чтение** в функциональной области **Общие функции → Базовая функциональность**.
   - право **Чтение** в функциональной области **Общие функции → Виртуальные Серверы администрирования**.

Приложение сохраняет измененные права пользователя в учетной записи администратора.

Чтобы назначить администратора нескольких виртуальных Серверов администрирования:

1. В главном окне приложения нажмите на имя основного Сервера администрирования.

2. На открывшейся странице перейдите на вкладку **Права доступа** и нажмите на кнопку **Назначить**.

   В открывшемся окне **Добавить пользователей или группы** установите флажок рядом с пользователем, которого вы хотите назначить администратором.

3. Вы можете перейти на вкладку **Группы**, чтобы выбрать группы пользователей.

4. Нажмите на кнопку **Далее**.

5. Выберите серверы, для которых вы хотите назначить администратора, и нажмите **Далее**.

   При выборе двух и более виртуальных серверов доступ к их основному Серверу администрирования будет предоставлен автоматически. В этом случае выбор невозможно будет отменить, не отменяя выбор соответствующих виртуальных серверов.

6. Выберите роли администратора, которые вы хотите назначить пользователю, если это необходимо.

   Если вы хотите назначить пользовательские роли для текущего Сервера администрирования, перейдите в свойства этого Сервера администрирования, нажмите **Назначить роли** и выберите пользовательские роли.

7. Нажмите на кнопку **Готово**, чтобы применить изменения.

Администратор с выбранными ролями теперь назначен нескольким виртуальным Серверам администрирования.

Чтобы отозвать права доступа администратора:

1. Переключитесь на нужный Сервер администрирования.
2. В главном окне приложения нажмите на имя Сервера администрирования.
3. На открывшейся странице выберите вкладку **Права доступа**.
4. Установите флажок рядом с пользователем, у которого вы хотите отозвать права доступа.
5. Нажмите **Отозвать** и подтвердите действие.

Права доступа выбранного пользователя отозваны.

Настройка прав доступа с помощью назначения пользовательских ролей

Также вы можете предоставить права доступа администратору виртуального Сервера администрирования через пользовательскую роль. Например, это может быть полезно, если вы хотите назначить несколько администраторов на один и тот же виртуальный Сервер администрирования. В этом случае вы можете назначить учетным записям администраторов одну или несколько пользовательских ролей вместо того, чтобы настраивать одни и те же права для нескольких администраторов.

Чтобы назначить администратора виртуального Сервера администрирования, назначив ему пользовательские роли:

1. На главном Сервере администрирования создайте пользовательскую роль и укажите все необходимые права доступа, которыми должен обладать администратор на виртуальном Сервере администрирования. Вы можете создать несколько ролей, например, если хотите разделить доступ к разным функциональным областям.
2. Переключитесь на нужный виртуальный Сервер администрирования:
   a. В главном меню выберите раздел (кроме **Marketplace**, **Навигация консоли** и **Параметры**), а затем в верхней части страницы нажмите на кнопку **Показать иерархию**.
   b. В открывшейся панели нажмите на имя нужного виртуального Сервера администрирования.

   > Вы не можете переключиться на виртуальный Сервер администрирования из разделов **IP-диапазоны** и **Удаленные объекты**.

   В главном меню Сервер администрирования изменится на тот, который вы выбрали.
3. Назначьте новую роль или несколько ролей учетной записи администратора.

> При назначении ролей пользователю, в главном окне приложения перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**. Если вы выберете вкладку **Группы** и назначите роли группе, членом которой является пользователь, пользователь не сможет войти в Kaspersky Security Center Cloud Console.

Приложение назначает новую роль учетной записи администратора.

Настройка прав доступа на уровне объекта

В дополнение к назначению прав доступа на уровне функциональной области, вы можете настроить доступ к определенным объектам на виртуальном Сервере администрирования, например, к определенной группе администрирования или задаче. Для этого переключитесь на виртуальный Сервер администрирования, а затем настройте права доступа в свойствах объекта.

Удаление виртуального Сервера администрирования

При удалении виртуального Сервера администрирования все объекты, созданные на Сервере администрирования, включая политики и задачи, также будут удалены. Управляемые устройства из групп администрирования, которыми управлял виртуальный Сервер администрирования, будут удалены из групп администрирования. Чтобы вернуть устройства под управление Kaspersky Next XDR Expert, выполните опрос сети, а затем переместите найденные устройства из группы Нераспределенные устройства в группы администрирования.

Чтобы удалить виртуальный Сервер администрирования:

1. В главном окне приложения нажмите на Сервер администрирования.
2. На открывшейся странице перейдите на вкладку **Серверы администрирования**.
3. Выберите виртуальный Сервер администрирования, который вы хотите удалить.
4. В строке меню нажмите на кнопку **Удалить**.

Виртуальный Сервер администрирования удален.

Удаленная диагностика клиентских устройств

Вы можете использовать удаленную диагностику для удаленного выполнения следующих операций на клиентских устройствах на базе Windows и на базе Linux:

- включения и выключения трассировки, изменения уровня трассировки и загрузки файла трассировки;
- загрузки системной информации и параметров приложения;
- загрузки журналов событий;
- создание файла дампа для приложения;
- запуска диагностики и загрузки результатов диагностики;
- запуск, остановка и перезапуск приложений.

Вы можете использовать журнал событий и диагностические отчеты, загруженные с клиентского устройства, для устранения неполадок самостоятельно. Также если вы обращаетесь в Службу технической поддержки "Лаборатории Касперского", эксперт технической поддержки "Лаборатории Касперского" может попросить вас загрузить файлы трассировки, файлы дампа, журнал событий и диагностические отчеты с клиентского устройства для дальнейшего анализа в "Лаборатории Касперского".

Открытие окна удаленной диагностики

Чтобы выполнить удаленную диагностику клиентских устройств на базе Windows и на базе Linux, сначала нужно открыть окно удаленной диагностики.

Чтобы открыть окно удаленной диагностики:

1. Чтобы выбрать устройство, для которого вы хотите открыть окно удаленной диагностики, выполните одно из следующих действий:

   - Если устройство принадлежит к группе администрирования, в главном меню перейдите в раздел **Управление активами → Управляемые устройства**.

   - Если устройство принадлежит к группе нераспределенных устройств, в главном меню перейдите в раздел **Управление активами → Нераспределенные устройства**.

2. Нажмите на имя требуемого устройства.

3. В открывшемся окне свойств устройства выберите вкладку **Дополнительно**.

4. На вкладке **Дополнительно** нажмите **Удаленная диагностика**.

   В результате открывается окно **Удаленная диагностика** клиентского устройства. Если отсутствует соединение между Сервером администрирования и клиентским устройством, появится сообщение об ошибке.

Если вам нужно получить сразу всю диагностическую информацию о клиентском устройстве с операционной системой Linux, вы можете запустить на этом устройстве скрипт collect.sh.

Включение и выключение трассировки для приложений

Вы можете включать и выключать трассировку для приложений, включая трассировку xperf.

Включение и выключение трассировки

Чтобы включить или выключить трассировку на удаленном устройстве:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В дереве объектов устройства выберите приложение, для которого требуется включить или выключить трассировку.

   Откроется список параметров удаленной диагностики.

4. Если вы хотите включить трассировку:

   a. В разделе **Трассировка** нажмите на кнопку **Включить трассировку**.

   b. В открывшемся окне **Изменить уровень трассировки** рекомендуется не менять значения, заданные по умолчанию. При необходимости эксперт Службы технической поддержки проведет вас через процесс настройки. Доступны следующие параметры:

   - **Уровень трассировки**

     Уровень трассировки определяет состав информации, которую содержит файл трассировки.

   - **Трассировка на основе ротации**

     Приложение перезаписывает информацию трассировки, чтобы предотвратить чрезмерное увеличение файла трассировки. Укажите максимальное количество файлов, которые будут использоваться для хранения информации трассировки, и максимальный размер каждого файла. Если записано максимальное количество файлов трассировки максимального размера, самый старый файл трассировки будет удален, чтобы можно было записать новый файл трассировки.

     Этот параметр доступен только для Kaspersky Endpoint Security.

   c. Нажмите на кнопку **Сохранить**.

   Трассировка включена для выбранного приложения. В некоторых случаях для включения трассировки приложения безопасности требуется перезапустить это приложение и его задачу.

   > На клиентских устройствах под управлением Linux трассировка компонента Обновление Kaspersky Security Agent регулируется параметрами Агента администрирования. Поэтому параметры **Включить трассировку** и **Изменить уровень трассировки** выключены для этого компонента на клиентских устройствах под управлением Linux.

5. Если вы хотите выключить трассировку для выбранного приложения, нажмите на кнопку **Выключить трассировку**.

   Трассировка выключена для выбранного приложения.

Включение трассировки Xperf

Для Kaspersky Endpoint Security эксперты Службы технической поддержки могут попросить вас включить трассировку Xperf для получения информации о производительности системы.

Чтобы включить, настроить или отключить трассировку Xperf:

1. Откройте утилиту удаленной диагностики клиентского устройства.

2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.

3. В списке приложений выберите Kaspersky Endpoint Security для Windows.

   Откроется список параметров удаленной диагностики для Kaspersky Endpoint Security для Windows.

4. В разделе **Трассировка Xperf** нажмите на кнопку **Включить трассировку Xperf**.

   Если трассировка Xperf уже включена, отображается кнопка **Выключить трассировку Xperf**. Нажмите на эту кнопку, если хотите отключить трассировку Xperf для Kaspersky Endpoint Security для Windows.

5. В открывшемся окне **Изменить уровень трассировки Xperf**, в зависимости от запроса эксперта Службы технической поддержки, выполните следующее:

   a. Выберите один из уровней трассировки:

   - **Легкий уровень**

     Файл трассировки этого типа содержит минимальный объем информации о системе.

     По умолчанию выбран этот вариант.

   - **Детальный уровень**

     Файл трассировки этого типа содержит более подробную информацию, чем файл типа *Легкий уровень*, и может запрашиваться специалистами Технической поддержки, если информации в файле трассировки *легкого уровня* недостаточно для оценки производительности. Файл трассировки *Детального уровня* содержит информацию об оборудовании, операционной системе, список запущенных и завершенных процессов и приложений, событиях, используемых для оценки производительности, а также события Средства оценки системы Windows.

   b. Выберите один из уровней трассировки Xperf:

   - **Базовый тип**

     Приложение получает данные трассировки во время работы приложения Kaspersky Endpoint Security.

     По умолчанию выбран этот вариант.

   - **Тип перезагрузки**

     Приложение получает данные трассировки, когда на управляемом устройстве запускается операционная система. Этот тип трассировки эффективен, когда проблема, влияющая на производительность системы, возникает после включения устройства и перед запуском Kaspersky Endpoint Security.

   Также вам могут предложить включить параметр **Размер файлов ротации (МБ)**, чтобы предотвратить чрезмерное увеличение файла трассировки. Затем укажите максимальный размер файла трассировки. Когда файл достигает максимального размера, самый старый файл трассировки будет перезаписан новым файлом.

   c. Определите размер файла ротации.

   d. Нажмите на кнопку **Сохранить**.

   Трассировка Xperf включена и настроена.

6. Если вы хотите отключить трассировку Xperf для Kaspersky Endpoint Security для Windows, нажмите **Выключить трассировку Xperf** в разделе **Трассировка Xperf**.

   Трассировка Xperf выключена.

Загрузка файла трассировки приложения

Вы можете загрузить файлы трассировки с клиентского устройства только если выполняется одно из двух условий: либо параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, либо используется шлюз соединения. Иначе загрузка невозможна..

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

Чтобы загрузить файл трассировки приложения:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите приложение, для которого вы хотите загрузить файл трассировки.
4. В разделе **Трассировка** нажмите на кнопку **Файлы трассировки**.

   Откроется окно **Журналы удаленной установки**, где отображается список файлов трассировки.
5. В списке файлов трассировки выберите файл, который вы хотите загрузить.
6. Выполните одно из следующих действий:

   - Загрузите выбранный файл, нажав на кнопку **Скачать**. Вы можете выбрать один или несколько файлов для загрузки.
   - Загрузите часть выбранного файла:

     a. Нажмите на кнопку **Скачать часть**.

     Одновременная частичная загрузка нескольких файлов невозможна. Если вы выберете более одного файла трассировки, кнопка **Скачать часть** будет неактивна.

     b. В открывшемся окне укажите имя и часть файла для загрузки в соответствии с вашими требованиями.

     Для устройств под управлением Linux изменение имени части файла недоступно.

     c. Нажмите на кнопку **Скачать**.

Выбранный файл или его часть загружается в указанное вами расположение.

Удаление файлов трассировки

Вы можете удалить файлы трассировки, которые больше не нужны.

Чтобы удалить файл трассировки, выполните следующее действие:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В открывшемся окне удаленной диагностики выберите раздел **Журналы событий**.
3. В разделе **Файлы трассировки** нажмите **Журналы службы Центра обновления Windows** или **Журналы удаленной установки**, в зависимости от того, какие файлы трассировки вы хотите удалить.

   Откроется окно **Журналы удаленной установки**, где отображается список файлов трассировки.
4. В списке файлов трассировки выберите один или несколько файлов, которые вы хотите удалить.
5. Нажмите на кнопку **Удалить**.

Выбранные файлы трассировки удалены.

Загрузка параметров приложений

Вы можете загрузить параметры приложений с клиентского устройства только если выполняется одно из двух условий: либо параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, либо используется шлюз соединения. Иначе загрузка невозможна.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

Чтобы загрузить с клиентского устройства параметры программ:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.
3. В разделе **Параметры приложения** нажмите на кнопку **Скачать** для загрузки информации о параметрах приложений, установленных на клиентском устройстве.

ZIP-архив с информацией загрузится в указанное расположение.

Загрузка системной информации с клиентского устройства

Вы можете загрузить системную информацию с клиентского устройства на свое устройство только если выполняется одно из двух условий: либо параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, либо используется шлюз соединения. Иначе загрузка невозможна.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

Чтобы загрузить системную информацию с клиентского устройства выполните следующие действия:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Информация о системе**.

3. Нажмите на кнопку **Скачать** для загрузки системной информации о клиентском устройстве.

> Архив может содержать конфиденциальные данные (например, ключи и пароли) в виде обычного текста. Рекомендуется просмотреть файлы в архиве и удалить такие данные перед отправкой в Службу технической поддержки "Лаборатории Касперского".

Файл с информацией загрузится в указанное расположение.

Загрузка журналов событий

Вы можете загружать журналы событий с клиентского устройства на свое устройство только если выполняется одно из двух условий: либо параметр **Не разрывать соединение с Сервером администрирования** включен в параметрах устройства, либо используется шлюз соединения. Иначе загрузка невозможна.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

Чтобы загрузить с удаленного устройства журнал событий:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В разделе **Журналы событий** в окне удаленной диагностики выберите **Все журналы устройства**.
3. В окне **Все журналы событий устройства** выберите один или несколько журналов событий.
4. Выполните одно из следующих действий:
   - Загрузите выбранный журнал событий, нажав на кнопку **Скачать весь файл**.
   - Загрузите часть выбранного журнала событий:
     a. Нажмите на кнопку **Скачать часть**.

        Одновременная частичная загрузка нескольких журналов событий невозможна. Если вы выберете более одного журнала событий, кнопка **Скачать часть** будет неактивна.

     b. В открывшемся окне укажите имя и часть журнала событий для загрузки в соответствии с вашими требованиями.

     c. Нажмите на кнопку **Скачать**.

Выбранный журнал событий или его часть загрузится в указанное расположение.

Запуск, остановка и перезапуск приложения

Вы можете запускать, останавливать и перезапускать приложения на клиентском устройстве.

Чтобы запустить, остановить или перезапустить приложение:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите приложение, которое вы хотите запустить, остановить или перезапустить.
4. Выберите действие, нажав на одну из следующих кнопок:

   - **Остановить приложение**

     Эта кнопка доступна, только если приложение в данный момент запущено.
   - **Перезапустить приложение**

     Эта кнопка доступна, только если приложение в данный момент запущено.
   - **Запустить приложение**

     Эта кнопка доступна, только если приложение в данный момент не запущено.

В зависимости от выбранного вами действия требуемое приложение запустится, остановится или перезапустится на клиентском устройстве.

Если вы перезапустите Агент администрирования, появится сообщение о том, что текущее соединение устройства с Сервером администрирования будет потеряно.

Запуск удаленной диагностики приложения и загрузка результатов

Чтобы запустить диагностику приложения на удаленном устройстве и загрузить ее результаты:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите приложение, для которого вы хотите запустить удаленную диагностику.

   Откроется список параметров удаленной диагностики.
4. В разделе **Отчет диагностики** нажмите на кнопку **Выполнить диагностику**.

   Запускается процесс удаленной диагностики и генерируется отчет о диагностике. После завершения процесса диагностики кнопка **Скачать отчет диагностики** становится доступной.
5. Нажмите на кнопку **Скачать отчет диагностики**, чтобы загрузить отчет.

Отчет загрузится в указанное расположение.

Запуск приложения на клиентском устройстве

Вам может потребоваться запустить приложение на клиентском устройстве, если вас об этом попросит специалист Службы технической поддержки "Лаборатории Касперского". Вам не нужно устанавливать приложение самостоятельно на этом устройстве.

Если вы хотите запустить пользовательский скрипт на клиентском устройстве, вы можете использовать переменную среды `KLACDT_SAVE_SETTING`, чтобы определить путь, по которому будут сохранены результаты выполнения. Например:

- Для устройств с операционной системой Windows:

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```

- Для устройств с операционной системой Linux:

  ```
  echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

Чтобы запустить приложение на клиентском устройстве:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Запуск удаленного приложения**.
3. В поле **Тип объекта** выберите тип объекта, который вы хотите загрузить:
   - Выберите **Файл** для загрузки исполняемого файла.
   - Выберите **Папка** для загрузки папки, содержащей приложение, которое вы хотите запустить на клиентском устройстве.

     Если вы выберете этот тип объекта, отобразится поле **Имя исполняемого файла, который будет запущен**. В этом поле укажите имя исполняемого файла в папке. Также можно указать относительный путь к файлу.
   - Выберите **Архив** для загрузки ZIP-архива, содержащего приложение, которое вы хотите запустить на клиентском устройстве.

     Если вы выберете этот тип объекта, отобразится поле **Имя исполняемого файла, который будет запущен**. В этом поле укажите имя исполняемого файла в папке, который вы хотите запустить на клиентском устройстве. Также можно указать относительный путь к файлу.

     > ZIP-архив должен содержать папку утилиты. Эта папка содержит исполняемый файл для запуска на удаленном устройстве.
4. Загрузите объект, выбрав его в системном окне или перетащив его в поле загрузки.
5. При необходимости в поле **Аргументы командной строки** укажите аргументы командной строки, которые будут переданы при запуске исполняемого файла.
6. Нажмите на кнопку **Загрузить и запустить** для запуска выбранного приложения на клиентском устройстве.

7. После успешного выполнения приложения, загрузите результаты выполнения, нажав на кнопку **Скачать результаты выполнения приложения**.

   Результаты выполнения приложения хранятся до тех пор, пока вы не запустите новую диагностику или не закроете окно.

Удаленная диагностика клиентского устройства с использованием приложения завершена.

Создание файла дампа для приложения

Файл дампа приложения позволяет просматривать параметры приложения, работающего на клиентском устройстве, в определенный момент времени. Этот файл также содержит информацию о модулях, которые были загружены для приложения.

Создание файлов дампа доступно только для 32-разрядных процессов, работающих на клиентских устройствах под управлением Windows. Для клиентских устройств под управлением Linux и для 64-битных процессов эта функция не поддерживается.

Чтобы создать файл дампа для приложения:

1. Откройте утилиту удаленной диагностики клиентского устройства.
2. В окне удаленной диагностики выберите раздел **Запуск удаленного приложения**.
3. В разделе **Формирование файла дампа процесса** укажите исполняемый файл приложения, для которого вы хотите создать файл дампа.
4. Нажмите на кнопку **Скачать**, чтобы сохранить файл дампа указанного приложения.

   Если указанное приложение не запущено на клиентском устройстве, отобразится сообщение об ошибке.

Запуск удаленной диагностики на клиентском устройстве с операционной системой Linux

Open Single Management Platform позволяет загружать основную диагностическую информацию с клиентского устройства. Также вы можете получить диагностическую информацию об устройстве с операционной системой Linux с помощью скрипта collect.sh "Лаборатории Касперского". Этот скрипт запускается на клиентском устройстве с операционной системой Linux, которое необходимо диагностировать. Затем создается файл с диагностической информацией, системной информацией об этом устройстве, файлами трассировки приложений, журналами событий устройства и файлом дампа для аварийных ситуаций, прерванных приложений.

Рекомендуется использовать скрипт collect.sh для получения сразу всей диагностической информации о клиентском устройстве с операционной системой Linux. Если вы загружаете диагностическую информацию удаленно через Open Single Management Platform, вам нужно будет пройти все разделы интерфейса удаленной диагностики. Также диагностическая информация для устройства с операционной системой Linux, вероятно, не будет получена полностью.

Если вам необходимо отправить сформированный файл с диагностической информацией в Службу технической поддержки "Лаборатории Касперского", удалите всю конфиденциальную информацию перед отправкой файла.

Чтобы загрузить диагностическую информацию с клиентского устройства с операционной системой Linux с помощью скрипта collect.sh:

1. Загрузите скрипт collect.sh, который запакован в архив collect.tar.gz.
2. Скопируйте загруженный архив на клиентское устройство с операционной системой Linux, которое необходимо диагностировать.
3. Выполните команду, чтобы распаковать архив collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Выполните команду, чтобы указать права на выполнение скрипта:

   ```
   # chmod +x collect.sh
   ```

5. Запустите сценарий collect.sh под учетной записью с правами администратора:

   ```
   # ./collect.sh
   ```

Файл с диагностической информацией будет сформирован и сохранен в папке /tmp/$HOST_NAME-collect.tar.gz.

Экспорт событий в SIEM-системы

В этом разделе описывается, как настроить экспорт событий в SIEM-системы.

Настройка экспорта событий в SIEM-системы

В этом разделе представлен сценарий настройки экспорта событий с Сервера администрирования во внешние SIEM-системы. Экспорт информации о событиях во внешние SIEM-системы позволяет администраторам SIEM-систем оперативно реагировать на события системы безопасности, произошедшие на управляемых устройствах или группах устройств.

Предварительные требования

Перед началом настройки экспорта событий в Kaspersky SIEM Cloud:

- Узнайте больше о методах экспорта событий.
- Убедитесь, что вам известны значения системных параметров.

Вы можете выполнять шаги этого сценария в любом порядке.

Этапы

Процесс экспорта событий в SIEM-систему состоит из следующих этапов:

- **Настройка SIEM-системы для получения событий из Kaspersky SIEM Cloud**

  Вам необходимо настроить получение событий из Kaspersky SIEM Cloud в SIEM-системе.

- **Выбор событий для экспорта**

  Вам нужно выбрать, какие события вы хотите экспортировать в SIEM-систему. Сначала отметьте общие события, которые происходят во всех управляемых приложениях "Лаборатории Касперского". Также можно отметить события для конкретных управляемых приложений "Лаборатории Касперского".

- **Настройка Kaspersky SIEM Cloud для экспорта событий в SIEM-систему**

  Вам необходимо настроить Kaspersky SIEM Cloud для начала экспорта событий в SIEM-систему.

Результаты

После настройки экспорта событий в SIEM-систему вы можете просматривать результаты экспорта, если вы выбрали события, которые хотите экспортировать.

Предварительные условия

При настройке автоматического экспорта событий в Kaspersky SIEM Cloud необходимо указать некоторые параметры SIEM-системы. Рекомендуется уточнить эти параметры заранее, чтобы подготовиться к настройке Kaspersky SIEM Cloud.

Для настройки автоматического экспорта событий в SIEM-систему необходимо знать значения следующих параметров:

- **Адрес сервера SIEM-системы**

  Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

- **Порт сервера SIEM-системы**

  Номер порта, по которому будет установлено соединение между Kaspersky SIEM Cloud и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky SIEM Cloud и настройках приемника в SIEM-системе.

- **Протокол**

  Протокол, используемый для передачи сообщений из Kaspersky SIEM Cloud в SIEM-систему. Это значение необходимо указать в настройках Kaspersky SIEM Cloud и настройках приемника в SIEM-системе.

Об экспорте событий

Kaspersky SIEM Cloud позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования.

Вы можете использовать экспорт событий в централизованных системах, работающих с вопросами безопасности на организационном и техническом уровнях, обеспечивающих мониторинг систем безопасности и консолидирующих данные из различных решений. К ним относятся SIEM-системы, обеспечивающие анализ алертов систем безопасности и событий сетевого аппаратного обеспечения и приложений в режиме реального времени, а также центры управления безопасностью (Security Operation Center, SOC).

SIEM-системы получают данные из многих источников, включая сети, системы безопасности, серверы, базы данных и приложения. Они также обеспечивают функцию объединения обработанных данных, что не позволит вам пропустить критические события. Кроме того, эти системы выполняют автоматический анализ связанных событий и сигналов тревоги для уведомления администраторов о вопросах системы безопасности, требующих незамедлительного решения. Уведомления могут отображаться в панели индикаторов или рассылаться по сторонним каналам, например, по электронной почте.

В процедуре экспорта событий из Kaspersky SIEM Cloud во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky SIEM Cloud и получатель событий – SIEM-система. Для успешного экспорта событий необходимо выполнить настройки и в используемой SIEM-системе, и в Консоли администрирования Kaspersky SIEM Cloud. Последовательность настройки не имеет значения: Вы можете либо сначала настроить отправку событий в Kaspersky SIEM Cloud, а затем получение событий в SIEM-системе, либо наоборот.

Экспорт событий в формате Syslog

Вы можете отправлять события в формате syslog в любую SIEM-систему. Используя формат Syslog, вы можете передавать любые события, произошедшие на Сервере администрирования и в приложениях "Лаборатории Касперского", установленных на управляемых устройствах. При экспорте событий в формате Syslog можно выбирать, какие именно события будут переданы в SIEM-систему. Получение событий SIEM-системой

Получение событий SIEM-системой

SIEM-система должна принимать и корректно анализировать события, получаемые из Kaspersky SIEM Cloud. Для этого необходимо правильно настроить SIEM-систему. Конфигурация зависит от конкретной используемой SIEM-системы. Однако в конфигурациях всех SIEM-систем существует ряд общих этапов, таких как настройка приемника и анализатора.

Настройка экспорта событий в SIEM-системе

В процедуре экспорта событий из Kaspersky SIEM Cloud во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky SIEM Cloud и получатель событий – SIEM-система. Экспорт событий необходимо настроить в используемой SIEM-системе и в Kaspersky SIEM Cloud.

Настройки, выполняемые в SIEM-системе, зависят от того, какую систему вы используете. В общем случае для всех SIEM-систем необходимо настроить приемник сообщений и, при необходимости, анализатор сообщений, для того чтобы разложить полученные сообщения на поля.

Настройка приемника сообщений

Для SIEM-системы необходимо настроить приемник для получения событий, отправляемых Kaspersky SIEM Cloud. В общем случае в SIEM-системе необходимо указать следующие параметры:

- **Порт**

  Укажите номер порта для подключения к Kaspersky SIEM Cloud. Этот порт должен совпадать с портом, который вы указываете в Kaspersky SIEM Cloud при настройке экспорта событий в SIEM-систему.

- **Протокол передачи сообщений или тип исходных данных**

  Укажите формат Syslog.

В зависимости от используемой SIEM-системы может потребоваться указать дополнительные параметры приемника сообщений.

Анализатор сообщений

Экспортируемые события передаются в SIEM-систему в виде сообщений. Затем к этим сообщениям применяется анализатор, для того чтобы информация о событиях была должным образом передана в SIEM-систему. Анализатор сообщений встроен в SIEM-систему; он используется для разбиения сообщения на поля, такие как идентификатор сообщения, уровень важности, описание и прочие параметры. В результате SIEM-система имеет возможность выполнять обработку событий, полученных из Kaspersky SIEM Cloud, таким образом, чтобы они сохранялись в базе данных SIEM-системы.

Выбор событий для экспорта в SIEM-системы в формате syslog

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться во внешнюю SIEM-систему.

Вы можете настроить экспорт событий в формате syslog во внешнюю систему на основе одного из следующих условий:

- Выбор общих событий. Если вы выберите экспортируемые события в политике, в свойствах события или в свойствах Сервера администрирования, то в SIEM-систему будут переданы выбранные события, которые произошли во всех приложениях, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельного приложения, управляемой этой политикой.

- Выбор событий для управляемого приложения. Если вы выбираете экспортируемые события для управляемого приложения, установленного на управляемых устройствах, то в SIEM-систему будут переданы только события, которые произошли в этом приложении.

Для событий изменения политик вы можете только включить или выключить экспорт всех таких событий в SIEM-систему.

Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog

Если вы хотите выполнить экспорт событий, произошедших в определенном управляемом приложении, установленном на управляемых устройствах, выберите события для экспорта политике приложения. В этом случае отмеченные события экспортируются со всех устройств, входящих в область действия политики.

Чтобы отметить события для экспорта для определенного управляемого приложения:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.

2. Выберите политику приложения, для которого нужно отметить события.

   Откроется окно свойств политики.

3. Перейдите в раздел **Настройка событий**.

4. Установите флажки рядом с событиями, которые требуется экспортировать в SIEM-систему.

5. Нажмите на кнопку **Отметить для экспорта в SIEM-систему по протоколу syslog**.

> Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

6. Флажок (✓) появляется в столбце **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.

7. Нажмите на кнопку **Сохранить**.

Отмеченные события из управляемого приложения готовы к экспорту в SIEM-систему.

Вы можете отметить, какие события экспортировать в SIEM-систему для конкретного управляемого устройства. В случае, если ранее экспортируемые события были выбраны в политике приложения, вам не удастся переопределить выбранные события для управляемого устройства.

Чтобы выбрать события для управляемого устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.

   Отобразится список управляемых устройств.

2. Перейдите по ссылке с названием требуемого устройства в списке управляемых устройств.

   Откроется окно свойств выбранного устройства.

3. Перейти в раздел **Приложения**.

4. Перейдите по ссылке с названием требуемого приложения в списке приложений.

5. Перейдите в раздел **Настройка событий**.

6. Установите флажки рядом с событиями, которые требуется экспортировать в SIEM-систему.

7. Нажмите на кнопку **Отметить для экспорта в SIEM-систему по протоколу syslog**.

   Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

8. Флажок (✓) появляется в столбце **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.

Теперь Сервер администрирования отправляет в SIEM-систему выбранные события, если экспорт в SIEM-систему настроен.

Выбор общих событий для экспорта в формате Syslog

Вы можете отметить общие события, которые Сервер администрирования будет экспортировать в SIEM-системы, используя формат syslog.

Чтобы выбрать общие события для экспорта в SIEM-систему:

1. Выполните одно из следующих действий:

   - В главном окне приложения нажмите на имя Сервера администрирования.
   - В главном окне приложения перейдите в раздел **Управление активами** → **Политики**, а затем перейдите по ссылке политики.

2. В открывшемся окне выберите вкладку **Настройка событий**.

3. Нажмите **Отметить для экспорта в SIEM-систему по протоколу syslog**.

   Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

4. Флажок (✓) появляется в столбце **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.

Теперь Сервер администрирования отправляет в SIEM-систему выбранные события, если экспорт в SIEM-систему настроен.

Об экспорте событий в формате Syslog

Используя формат Syslog можно выполнять экспорт в SIEM-системы событий, произошедших на Сервере администрирования и в других приложениях "Лаборатории Касперского", установленных на управляемых устройствах.

Syslog – это стандартный протокол регистрации сообщений. Этот протокол позволяет разделить программное обеспечение, генерирующее сообщения, систему, в которой хранятся сообщения, и программное обеспечение, выполняющее анализ и отчетность по сообщениям. Каждому сообщению присваивается код устройства, указывающий тип программного обеспечения, с помощью которого было создано сообщение, и уровень важности.

Формат Syslog определяется документами Request for Comments (RFC), опубликованными Internet Engineering Task Force. Стандарт RFC 5424 используется для экспорта событий из Kaspersky SIEM Cloud во внешние системы.

В Kaspersky SIEM Cloud можно настроить экспорт событий во внешние системы в формате Syslog.

Процесс экспорта состоит из двух шагов:

1. Включение автоматического экспорта событий. На этом шаге выполняется настройка Kaspersky SIEM Cloud таким образом, чтобы выполнялась отправка событий в SIEM-систему. Отправка событий из Kaspersky SIEM Cloud начинается сразу после включения автоматического экспорта.

2. Выбор событий, которые будут экспортироваться во внешнюю систему. На этом шаге вам нужно выбрать, какие события будут экспортироваться в SIEM-систему.

Настройка Kaspersky SIEM Cloud для экспорта событий в SIEM-систему

Для экспорта событий в SIEM-систему необходимо настроить процесс экспорта в Kaspersky SIEM Cloud.

Чтобы настроить экспорт в SIEM-системы из OSMP Console:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Перейдите в раздел **SIEM** и нажмите ссылку **Настроить подключения**.

3. На открывшейся правой панели **настройте параметры экспорта**.

- В поле **Адрес сервера SIEM-системы** укажите IP-адрес сервера, на котором установлена используемая SIEM-система.

  Это значение необходимо уточнить в настройках SIEM-системы.

- В поле **Порт SIEM-системы** укажите номер порта, по которому будет установлено соединение между Kaspersky SIEM Cloud и сервером SIEM-системы.

  Это значение необходимо указать в настройках Kaspersky SIEM Cloud и настройках приемника в SIEM-системе.

- В списке **Протокол** значение выбрано по умолчанию. Вы можете использовать только TLS over TCP для передачи сообщений в SIEM-систему.

- В раскрывающемся списке **Аутентификация Сервера** выберите одно из следующих значений:

  - **Доверенные сертификаты**, а затем нажмите отобразившуюся кнопку **Выбрать файл центра сертификации** для загрузки доверенного сертификата.

    Вы можете получить полную цепочку сертификатов (включая корневой сертификат) от доверенного центра сертификации (CA) и загрузить его в Kaspersky SIEM Cloud. Kaspersky SIEM Cloud проверяет, подписана ли цепочка сертификатов SIEM-системы также доверенным центром сертификации или нет.

  - **Отпечатки SHA**, а затем в поле **Отпечатки** введите отпечаток SHA1 и нажмите на кнопку **Добавить**.

    Вы можете указать отпечатки SHA1 всей цепочки сертификатов SIEM-системы (включая корневой сертификат) в Kaspersky SIEM Cloud.

- Перейдите по ссылке **Добавить имя субъекта/альтернативное имя субъекта**.

  > Эта ссылка отображается только в случае выбора пункта **Доверенные сертификаты** в раскрывающемся списке **Аутентификация Сервера**.

  Имя субъекта – это доменное имя, для которого получен сертификат. Kaspersky SIEM Cloud не может подключиться к серверу SIEM-системы, если доменное имя сервера SIEM-системы не совпадает с именем субъекта сертификата сервера SIEM-системы. Однако сервер SIEM-системы может изменить свое доменное имя, если имя изменилось в сертификате. В этом случае вы можете указать имена субъектов в поле **Имя субъекта/альтернативное имя субъекта**. Если какое-либо из указанных имен субъектов совпадает с именем субъекта сертификата SIEM-системы, Kaspersky SIEM Cloud проверяет сертификат сервера SIEM-системы.

- Перейдите по ссылке **Добавить проверку подлинности клиента**, а затем выберите в раскрывающемся списке **Если у вас нет сертификата, вы можете его сгенерировать** один из следующих вариантов:

  - **Сгенерировать ключ**, а затем нажмите на кнопку **Сгенерировать**, если требуется сгенерировать самоподписанный сертификат в Open Single Management Platform. В результате Kaspersky SIEM Cloud сохраняет сгенерированный самоподписанный сертификат, и вы можете передать публичную часть сертификата или SHA1-отпечаток в SIEM-систему.

    С помощью этого параметра вы можете сгенерировать сертификат для аутентификации Open Single Management Platform. Таким образом, вы будете использовать самоподписанный сертификат, выпущенный Open Single Management Platform. В этом случае для аутентификации сервера SIEM-системы можно использовать как доверенный сертификат, так и отпечаток SHA.

  - **Вставить сертификат**, если вы хотите использовать сертификат, полученный из любого источника, например от любого аккредитованного центра сертификации.

    Затем укажите сертификат с соответствующим закрытым ключом, выполнив следующие действия:

    a. В раскрывающемся списке **Сертификация клиента** выберите тип сертификата:

    - **X.509-сертификат PEM**
    - **X.509-сертификат PKCS12**

    b. В поле **Файл с сертификатом** загрузите файл с сертификатом.

    c. Если выбран вариант **X.509-сертификат PEM**, в отобразившемся разделе **Файл с ключом** загрузите файл с закрытым ключом.

    Файл с сертификатом и файл с закрытым ключом не зависят друг от друга, и порядок загрузки этих файлов не важен.

    d. Если закрытый ключ зашифрован, укажите пароль для расшифровки в поле **Проверка пароля или сертификата**. В противном случае это поле можно оставить пустым.

- В разделе **Формат данных** предварительно выбрано значение **Системный журнал**.

  Вы можете задать только ограничение длины сообщения, отправляемого в SIEM-систему, в поле **Максимальный размер сообщения в байтах**. В случае превышения этого предела сообщение будет обрезано.

4. Заархивированные события можно экспортировать из базы данных Сервера администрирования и задать начальную дату, с которой вы хотите начать экспорт заархивированных событий:

   a. Перейдите по ссылке **Установите дату начала экспорта**.

   b. В открывшемся разделе, укажите дату начала экспорта в поле **Дата начала экспорта**.

   c. Нажмите на кнопку **ОК**.

5. Включите параметр **Экспортировать события в SIEM**.

6. Чтобы отправлять события изменения политик в SIEM, включите параметр **Экспорт расширенных событий для изменений политики в SIEM**. Для каждого измененного параметра политики будет отправлено отдельное событие в SIEM.

7. Чтобы убедиться, что соединение с SIEM-системой настроено, нажмите на кнопку **Проверить подключение**.

   Отобразится статус подключения.

8. Нажмите на кнопку **Сохранить**.

Экспорт в SIEM-систему настроен. Если вы настроили получение событий в SIEM-системе, Сервер администрирования экспортирует выбранные события в SIEM-систему. Если вы установите дату начала экспорта, Сервер администрирования также экспортирует выбранные события, хранящиеся в базе данных Сервера администрирования, с указанной даты.

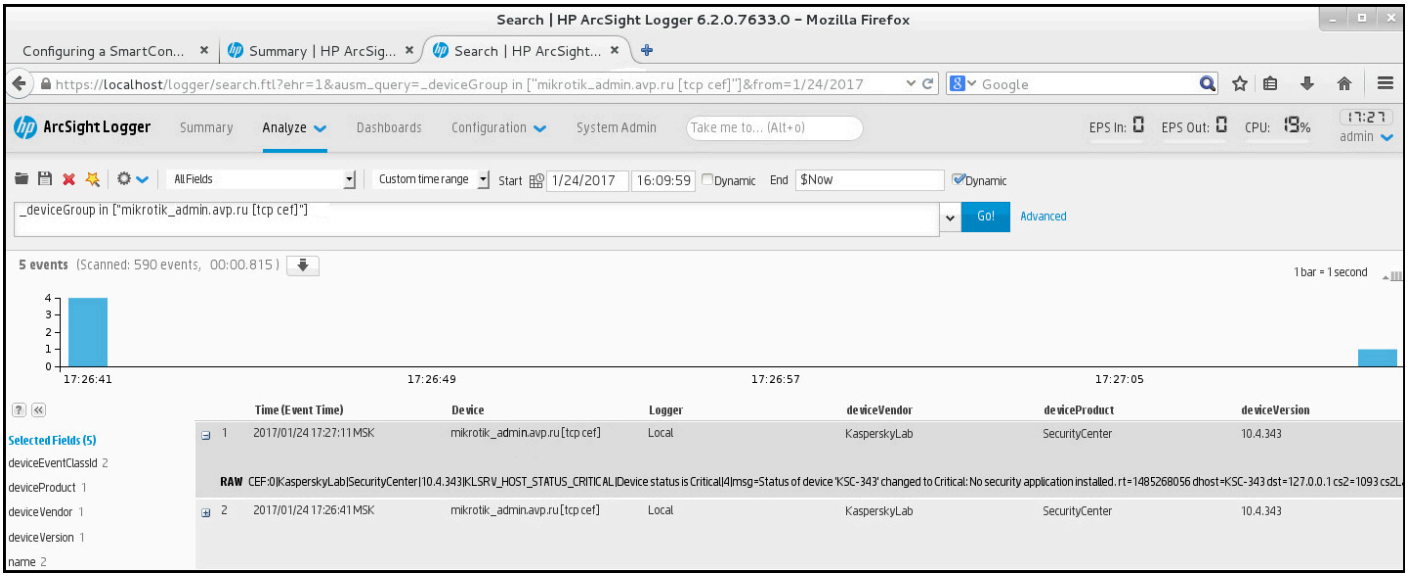
Просмотр результатов экспорта

Вы можете узнать, успешно ли завершилась процедура экспорта. Для этого проверьте, были ли получены SIEM-системой сообщения, содержащие экспортируемые события.

Если отправленные из Kaspersky SIEM Cloud события получены и правильно интерпретированы SIEM-системой, значит, настройка на обеих сторонах выполнена корректно. В противном случае проверьте и при необходимости исправьте настройки Kaspersky SIEM Cloud и SIEM-системы.

Ниже приведен пример событий, экспортированных в систему ArcSight. Например, первое событие – это критическое событие Сервера администрирования: *Статус устройства "Критический"*.

Отображение экспортированных событий зависит от используемой SIEM-системы.



Пример событий

Работа с Kaspersky Security Center Cloud Console в облачном окружении

В этом разделе представлена информация о функциях Kaspersky Security Center Cloud Console, связанных с эксплуатацией и обслуживанием Open Single Management Platform в облачных окружениях, таких как Amazon Web Services, Microsoft Azure и Google Cloud.

Для работы в облачном окружении вам нужна специальная лицензия. Если у вас нет такой лицензии, элементы интерфейса, связанные с облачными устройствами, не работают.

Updates functionality (including providing anti-virus signature updates and codebase updates), as well as KSN functionality may not be available in the software in the U.S.

Варианты лицензирования в облачном окружении

Работа в облачном окружении возможна как в пробном, так и в коммерческом режиме Kaspersky Security Center Cloud Console:

- В пробном режиме все функции облачного окружения доступны в течение всего срока действия вашей рабочей области. Лицензия не требуется.
- В коммерческом режиме возможности облачного окружения доступны только в том случае, если лицензионный ключ Kaspersky Security для виртуальных и облачных сред добавлен как активный в свойствах Сервера администрирования.

В обоих случаях автоматически активируется Системное администрирование.

Если возникает ошибка при попытке активировать функцию Поддержка облачного окружения с использованием лицензии Kaspersky Security для виртуальных и облачных сред, используйте файл ключа.

Подготовка к работе в облачном окружении с помощью Kaspersky Security Center Cloud Console

В этом разделе описано, как подготовиться к работе с Kaspersky Security Center Cloud Console в следующих облачных окружениях:

- Amazon Web Services;
- Microsoft Azure;
- Google Cloud.

Работа в облачном окружении Amazon Web Services

В этом разделе описано, как подготовиться к работе с Kaspersky Security Center Cloud Console в Amazon Web Services.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky Security Center Cloud Console.

О работе в облачном окружении Amazon Web Services

Для работы с платформой AWS, и в частности для того, чтобы создавать инстансы, вам потребуется учетная запись в Amazon Web Services. Вы можете создать бесплатную учетную запись на сайте https://aws.amazon.com/ru. Вы также можете использовать существующую учетную запись Amazon.

О том, что такое образы AMI и как работает магазин приложений AWS Marketplace, см. на странице справки AWS Marketplace. О работе с платформой AWS, об использовании инстансов и о связанных с ними понятиях см. в документации Amazon Web Services.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky SIEM Cloud.

Создание учетных записей IAM-пользователя для инстансов Amazon EC2

В этом разделе описано, какие действия необходимо выполнить, чтобы обеспечить корректную работу Kaspersky Security Center Cloud Console. Эти действия включают работу с сервисами AWS с учетными записям IAM-пользователей (Identity and Access Management). Также описано, какие действия должны быть выполнены с клиентскими устройствами, чтобы установить на них Агент администрирования и затем защитные приложения Kaspersky Endpoint Security для Linux.

Обеспечение прав для работы Kaspersky SIEM Cloud с AWS

Для работы в облачном окружении Amazon Web Services с помощью Kaspersky SIEM Cloud необходимо создать *учетную запись IAM-пользователя*, которую Kaspersky SIEM Cloud будет использовать для работы с сервисами AWS. Прежде чем начинать работу с Сервером администрирования, создайте учетную запись IAM-пользователя с *ключом доступа AWS IAM* (далее также *ключ доступа IAM*).

Для создания IAM-пользователя требуется Консоль управления AWS. Для работы с Консолью управления AWS вам понадобятся имя пользователя и пароль от учетной записи в AWS.

Создание учетной записи IAM-пользователя для работы Kaspersky SIEM Cloud

Учетная запись IAM-пользователя необходима для работы с Kaspersky SIEM Cloud. Вы можете создать одну учетную запись IAM-пользователя с требуемыми правами или две разные учетные записи.

Для IAM-пользователя автоматически создается *ключ доступа IAM*, который вам потребуется предоставить Kaspersky SIEM Cloud на этапе первоначальной настройки. Ключ доступа IAM состоит из ID ключа доступа и секретного ключа. Подробнее о службе IAM см. на следующих справочных страницах AWS:

- https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.
- https://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

Чтобы создать учетную запись IAM-пользователя с необходимыми правами:

1. Откройте Консоль управления AWS и войдите под своей учетной записью.
2. В списке служб AWS выберите **IAM**.

   Откроется окно, содержащее список имен пользователей и меню, с помощью которого вы сможете работать с инструментом.

3. Перейдите к областям консоли, использующим учетные записи пользователей, и добавьте новое имя пользователя или имена.

4. Для пользователей, которых вы добавили, укажите следующие параметры AWS:

   - Тип доступа: **Programmatic Access**.
   - Границы разрешений не установлены.
   - Разрешение: **ReadOnlyAccess**.

     После добавления разрешения просмотрите его на предмет точности. В случае ошибки выбора параметров перейдите к предыдущему экрану и выполните выбор параметров снова.

5. После того как вы создали учетную запись, отобразится таблица с ключом доступа IAM нового IAM-пользователя. ID ключа доступа отобразится в столбце **Access key ID**. Секретный ключ отобразится в столбце **Secret access key** в виде звездочек. Чтобы посмотреть секретный ключ, нажмите **Show**.

Созданная учетная запись отобразится в списке учетных записей IAM-пользователей, соответствующих вашей учетной записи в AWS.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky SIEM Cloud.

Работа в облачном окружении Microsoft Azure

В этом разделе представлена информация о том, как работать с Kaspersky SIEM Cloud в облачном окружении, предоставленном платформой Microsoft Azure, и как развернуть защиту на виртуальных машинах внутри облачного окружения.

О работе в Microsoft Azure

Чтобы работать с платформой Microsoft Azure, в частности для покупки приложений в магазине Azure Marketplace и создания виртуальных машин, вам потребуется подписка Azure. Перед тем как начать работу с Microsoft Azure в Kaspersky SIEM Cloud, создайте ID приложения в Azure с правами, необходимыми для установки приложения на виртуальные машины.

Создание подписки, идентификатора приложения и пароля

Для работы с Kaspersky SIEM Cloud в окружении Microsoft Azure вам нужны подписка Azure, ID приложения в Azure и пароль приложения в Azure. Вы можете использовать существующую подписку, если у вас она уже есть.

Подписка Azure предоставляет владельцу доступ к Microsoft Azure Platform Management Portal и сервисам Microsoft Azure. Владелец может использовать Microsoft Azure Platform, чтобы управлять службами, такими как Azure SQL и Azure Storage.

Чтобы создать подписку Microsoft Azure,

Перейдите по ссылке https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription и следуйте инструкциям.

Подробная информация о создании подписки доступна на сайте Microsoft. Вы получите идентификатор подписки, который затем предоставите Kaspersky SIEM Cloud вместе с ID приложения и паролем.

Чтобы создать и сохранить ID приложения и пароль Azure:

1. Перейдите по ссылке https://portal.azure.com и убедитесь, что выполнен вход.
2. Следуя инструкциям на странице справки, создайте ID приложения.
3. В свойствах приложения перейдите в раздел **Keys**.
4. В разделе **Keys** заполните поля **Description** и **Expires** и оставьте поле **Value** пустым.
5. Нажмите на кнопку **Сохранить**.

   После того как вы нажмете на кнопку **Save**, система автоматически заполнит поле **Value** длинной последовательностью символов. Эта последовательность символов является вашим паролем приложения в Azure (например, yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=). Описание отображается так, как вы его указали.
6. Скопируйте пароль и сохраните его, чтобы позже вы смогли предоставить ID приложения и пароль в Kaspersky SIEM Cloud.

   Вы можете скопировать пароль только при его создании. Позже пароль больше не будет отображаться, и вы не сможете его восстановить.

Адреса веб-страниц, указанные в этом документе, верны на дату выпуска Kaspersky SIEM Cloud.

Назначение роли для ID приложения в Azure

Если требуется только обнаружить виртуальные машины с помощью процесса обнаружения устройств, ID приложения в Azure должна быть назначена роль Читатель (Reader). Если требуется не только обнаружить виртуальные машины, но и развернуть защиту с помощью Azure API, ваш ID приложения в Azure должен иметь роль Участник виртуальных машин (Virtual Machine Contributor).

Следуйте инструкциям, приведенным на веб-сайте Microsoft, чтобы назначить роль для ID приложения в Azure.

Работа в Google Cloud

Этот раздел содержит информацию о работе с Kaspersky SIEM Cloud в облачном окружении, предоставляемом Google.

API Google можно использовать для работы с Kaspersky SIEM Cloud на платформе Google Cloud. Требуется учетная запись Google. Дополнительную информацию вы можете найти в документации Google на странице https://cloud.google.com.

Вам нужно создать и предоставить Kaspersky SIEM Cloud следующие учетные данные:

- **Электронная почта клиента**

  Электронная почта клиента – это адрес электронной почты, который вы использовали для регистрации вашего проекта в Google Cloud.

- **Идентификатор проекта.**

  Идентификатор проекта – это идентификатор, полученный при регистрации проекта Google Cloud.

- **Закрытый ключ.**

  Закрытый ключ – это последовательность символов, которые вы получили в качестве закрытого ключа при регистрации проекта в Google Cloud. Вы можете скопировать и вставить эту последовательность, чтобы избежать ошибок.

Мастер настройки для работы в облачном окружении в Kaspersky Security Center Cloud Console

Чтобы настроить Kaspersky SIEM Cloud с использованием мастера настройки облачного окружения, вам потребуется следующее:

- Укажите учетные данные для облачного окружения:
  - IAM-роль, которой было предоставлено право опроса облачного сегмента, или учетная запись IAM-пользователя, которому было предоставлено право опроса облачного сегмента (для работы с Amazon Web Services);
  - идентификатор приложения в Azure, пароль и подписка (для работы с Microsoft Azure);
  - электронная почта клиента Google, идентификатор проекта и закрытый ключ (для работы с Google Cloud).
- Инсталляционные пакеты:
  - Агент администрирования для Windows
  - Агент администрирования для Linux
  - Kaspersky Endpoint Security for Linux
- Веб-плагин Kaspersky Endpoint Security for Linux.
- Хотя бы одно из следующего:
  - инсталляционный пакет и веб-плагин Kaspersky Endpoint Security for Windows (рекомендуется);
  - инсталляционный пакет и веб-плагин Kaspersky Security для Windows Server или Linux Server.

Если ваша рабочая область была создана с использованием лицензии Kaspersky Security для виртуальных и облачных сред, мастер настройки облачного окружения запускается автоматически при первом подключении к Kaspersky Security Center Cloud Console. Если вы пропустите мастер настройки облачного окружения, он будет запускаться при каждом подключении к Kaspersky Security Center Cloud Console, пока вы не выполните все шаги мастера.

Вы также можете запустить мастер настройки для работы в облачном окружении вручную в любое время.

Чтобы запустить мастер настройки для работы в облачном окружении вручную:

В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Настройка работы в облачном окружении**.

Запустится мастер настройки для работы в облачном окружении.

Приблизительное время работы с мастером составляет около пятнадцати минут.

Если вы не активировали Сервер администрирования по лицензии Kaspersky Security для виртуальных и облачных сред, вам нужно выполнить это на первом шаге мастера.

Шаг 1. Проверка требуемых плагинов и инсталляционных пакетов

Этот шаг не отображается, если у вас есть все необходимые веб-плагины и инсталляционные пакеты, перечисленные ниже.

Для настройки облачного окружения требуется наличие следующих компонентов:

- Инсталляционные пакеты:
  - Агент администрирования для Windows
  - Агент администрирования для Linux
  - Kaspersky Endpoint Security for Linux
- Веб-плагин Kaspersky Endpoint Security for Linux.
- Инсталляционный пакет и веб-плагин Kaspersky Endpoint Security for Windows.

Kaspersky Next XDR Expert автоматически определяет уже имеющиеся компоненты и перечисляет только те, которых не хватает. Загрузите перечисленные компоненты, нажав на кнопку **Выберите приложения для загрузки**, и выберите необходимые плагины и инсталляционные пакеты. После загрузки компонента вы можете использовать кнопку **Обновить**, чтобы обновить список отсутствующих компонентов.

Шаг 2. Выбор способа активации приложения

Этот шаг отображается, только если при создании рабочей области вы использовали лицензию, отличную от Kaspersky Security для виртуальных и облачных сред, и никогда не добавляли лицензионный ключ Kaspersky Security для виртуальных и облачных сред в поле активации Сервера администрирования. В этом случае вам необходимо активировать Сервер администрирования с использованием лицензии Kaspersky Security для виртуальных и облачных сред.

Шаг 3. Выбор облачного окружения и аутентификация

Задайте следующие параметры:

- **Облачное окружение**

  Выберите облачное окружение, в котором вы разворачиваете Kaspersky Security Center: AWS, Azure или Google Cloud.

  Если вы планируете работать с несколькими облачными окружениями, выберите одно облачное окружение и потом запустите мастер еще раз.

- **Название соединения**

  Введите имя для соединения. Название может содержать не более 256 символов. Допустимы только символы Юникод.

  Это имя будет также использоваться как имя группы администрирования для облачных устройств.

  Если вы планируете работать с несколькими облачными окружениями, возможно, вы захотите включить имя среды в название соединения, например, "Сегмент Azure", "Сегмент AWS" или "Сегмент Google".

Введите свои учетные данные, чтобы получить аутентификацию в облачном окружении, которое вы указали.

AWS

Если вы выбрали AWS в качестве типа облачного сегмента, используйте ключ доступа AWS IAM для дальнейшего опроса облачного сегмента. Введите следующие данные ключа:

- **ID ключа доступа**

  ID ключа доступа IAM – это последовательность из букв и цифр. Вы получили ID ключа при создании учетной записи IAM-пользователя.

  Поле доступно, если вы выбрали для авторизации ключ доступа AWS IAM, а не IAM-роль.

- **Секретный ключ**

  Секретный ключ, который вы получили с ID ключа доступа при создании учетной записи IAM-пользователя.

  Символы секретного ключа отображаются в виде звездочек. После того, как вы начали вводить секретный ключ, отображается кнопка **Показать**. Нажмите на эту кнопку и удерживайте ее необходимое вам время, чтобы просмотреть введенные символы.

  Поле доступно, если вы выбрали для авторизации ключ доступа AWS IAM, а не IAM-роль.

  Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

Azure

Если вы выбрали Azure в качестве типа облачного сегмента, укажите следующие параметры соединения, которые в дальнейшем будут использоваться для опроса облачного сегмента:

- **Идентификатор приложения в Azure**

  Вы создали этот идентификатор приложения на портале Azure.

  Вы можете указать только один идентификатор приложения в Azure для опроса и других целей. Если необходимо опрашивать другой сегмент Azure, вам нужно сначала удалить первый сегмент в существующем соединении Azure.

- **Идентификатор подписки Azure**

  Вы создали подписку на портале Azure.

- **Пароль приложения Azure**

  Вы получили пароль к идентификатору приложения при создании ID приложения в Azure.

  Символы пароля отображаются в виде звездочек. После того, как вы начали вводить пароль, отображается кнопка **Показать**. Нажмите и удерживайте эту кнопку, чтобы просмотреть введенные символы.

  Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

- **Имя учетной записи хранения Azure**

  Вы создали имя учетной записи хранения Azure для работы с Kaspersky SIEM Cloud.

- **Ключ доступа хранилища Azure**

  Вы получили пароль (ключ) при создании учетной записи хранения Azure для работы с Kaspersky SIEM Cloud.

  Ключ доступен в разделе "Overview of the Azure storage account" в подразделе "Keys".

  Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

Google Cloud

Если вы выбрали Google Cloud в качестве типа облачного сегмента, укажите следующие параметры соединения, которые в дальнейшем будут использоваться для опроса облачного сегмента:

- **Электронная почта клиента**

  Электронная почта клиента – это адрес электронной почты, который вы использовали для регистрации вашего проекта в Google Cloud.

- **ID проекта**

  Идентификатор проекта – это идентификатор, полученный при регистрации проекта Google Cloud.

- **Закрытый ключ**

  Закрытый ключ – это последовательность символов, которые вы получили в качестве закрытого ключа при регистрации проекта в Google Cloud. Вы можете скопировать и вставить эту последовательность, чтобы избежать ошибок.

  Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

Указанное соединение сохранится в параметрах приложения.

Мастер настройки для работы в облачном окружении дает возможность указать только один сегмент. В дальнейшем вы можете указывать и другие соединения для управления другими облачными сегментами.

Нажмите на кнопку **Далее**, чтобы продолжить.

Шаг 4. Опрос сегментов и настройка синхронизации с облачным окружением

На этом шаге начинается опрос облачного сегмента и автоматически создается специальная группа администрирования для облачных устройств. Устройства, обнаруженные при опросе, перемещаются в эту группу. Расписание опроса облачного сегмента настроено (по умолчанию каждые пять минут; вы можете изменить этот параметр позже).

Также создается правило автоматического перемещения **Синхронизация с облачным окружением**. При каждом последующем сканировании облачной сети обнаруженные виртуальные устройства будут перемещаться в соответствующую подгруппу внутри группы **Управляемые устройства\Cloud**.

Укажите параметр **Синхронизировать группы администрирования с облачной структурой**.

Если параметр включен, то в группе **Управляемые устройства** автоматически создается группа **Cloud** и запускается процесс обнаружения устройств в облачной сети. Инстансы и виртуальные машины, обнаруженные во время каждого сканирования облачной сети, перемещаются в группу Cloud. Структура подгрупп администрирования в этой группе соответствует структуре вашего облачного сегмента (в AWS зоны доступности и группы размещения не представлены в структуре; в Azure подсети не представлены в структуре). Устройства, не идентифицированные как инстансы в облачном окружении, находятся в группе **Нераспределенные устройства**. Такая структура групп позволяет устанавливать антивирусные приложения на инстансы с помощью задач групповой установки и настраивать разные политики для разных групп.

Если параметр выключен, то также создается группа **Cloud** и запускается процесс обнаружения устройств в облачной сети, однако в группе не создаются подгруппы, соответствующие структуре облачного сегмента. Все найденные инстансы находятся в группе администрирования **Cloud** и отображаются единым списком. Если в процессе работы с Kaspersky SIEM Cloud вам потребуется произвести синхронизацию, то вы сможете изменить свойства правила **Синхронизация с облачным окружением** и форсировать его. Применение правила перестраивает структуру групп внутри группы Cloud так, чтобы она соответствовала структуре вашего облачного сегмента.

По умолчанию параметр выключен.

Нажмите на кнопку **Далее**, чтобы продолжить.

Шаг 5. Настройка Kaspersky Security Network для Kaspersky SIEM Cloud

Этот шаг пропускается при запуске Kaspersky SIEM Cloud в пробном режиме или на виртуальном Сервере администрирования.

Настройте параметры передачи информации о работе Open Single Management Platform в базу знаний Kaspersky Security Network (KSN). Выберите один из следующих вариантов:

- **Я принимаю условия использования Kaspersky Security Network**

  Kaspersky SIEM Cloud и управляемые приложения, установленные на клиентских устройствах, в автоматическом режиме будут предоставлять информацию об их работе Kaspersky Security Network. Сотрудничество с Kaspersky Security Network обеспечивает более быстрое обновление баз данных о вирусах и угрозах, что увеличивает скорость реагирования на возникающие угрозы безопасности.

- **Я не принимаю условия использования Kaspersky Security Network**

  Kaspersky SIEM Cloud и управляемые приложения не будут предоставлять информацию о своей работе Kaspersky Security Network.

  Если вы выбрали этот параметр, использование Kaspersky Security Network будет выключено.

"Лаборатория Касперского" рекомендует участие в Kaspersky Security Network.

Также могут отображаться Положения KSN для управляемых приложений. Если вы принимаете условия использования Kaspersky Security Network, управляемое приложение отправляет данные в "Лабораторию Касперского". Если вы не принимаете условия использования Kaspersky Security Network, управляемое приложение не будет отправлять данные в "Лабораторию Касперского". Этот параметр можно изменить позже в свойствах политики приложения.

Нажмите на кнопку **Далее**, чтобы продолжить.

Шаг 6. Создание первоначальной конфигурации защиты

Вы можете проверить список созданных политик и задач.

Дождитесь завершения создания политик и задач и нажмите на кнопку **Далее**, чтобы продолжить. На последней странице мастера нажмите на кнопку **Готово** для выхода.

Опрос сегмента сети с помощью Kaspersky Security Center Cloud Console

Информацию о структуре сети и входящих в ее состав устройствах получает в ходе регулярных опросов облачных сегментов средствами AWS API, Azure API или Google API. На основании полученной информации Kaspersky Security Center Cloud Console обновляет состав и содержимое папок Нераспределенные устройства и Управляемые устройства. Если вы настроили автоматическое перемещение устройств в группы администрирования, обнаруженные в сети устройства включаются в состав групп администрирования.

Чтобы разрешить опрос облачных сегментов, необходимы соответствующие права, которые обеспечивает учетная запись IAM-пользователя (в AWS), идентификатор приложения и пароль (в Azure) или адрес электронной почты клиента Google, идентификатор проекта Google и закрытый ключ (в Google Cloud).

Вы можете добавлять и удалять соединения, а также настраивать для каждого облачного сегмента расписание опроса.

Добавление подключений для опроса облачных сегментов через Kaspersky Security Center Cloud Console

Чтобы добавить соединение для опроса облачных сегментов в список доступных:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Cloud**.

2. В появившемся окне нажмите **Свойства**.

3. В появившемся окне **Параметры** нажмите на кнопку **Добавить**.

   Откроется окно **Параметры облачного сегмента**.

4. Укажите имя облачного окружения для соединения, которое в дальнейшем будет использоваться для опроса облачного сегмента:

   - **Облачное окружение**

     Выберите облачное окружение, в котором вы разворачиваете Kaspersky Security Center: AWS, Azure или Google Cloud.

     Если вы планируете работать с несколькими облачными окружениями, выберите одно облачное окружение и потом запустите мастер еще раз.

   - **Название соединения**

     Введите имя для соединения. Название может содержать не более 256 символов. Допустимы только символы Юникод.

     Это имя будет также использоваться как имя группы администрирования для облачных устройств.

     Если вы планируете работать с несколькими облачными окружениями, возможно, вы захотите включить имя среды в название соединения, например, "Сегмент Azure", "Сегмент AWS" или "Сегмент Google".

5. Введите свои учетные данные, чтобы получить аутентификацию в облачном окружении, которое вы указали.

   - Если вы выбрали AWS, укажите следующее:

     - **ID ключа доступа**

       ID ключа доступа IAM – это последовательность из букв и цифр. Вы получили ID ключа при создании учетной записи IAM-пользователя.

       Поле доступно, если вы выбрали для авторизации ключ доступа AWS IAM, а не IAM-роль.

     - **Секретный ключ**

       Секретный ключ, который вы получили с ID ключа доступа при создании учетной записи IAM-пользователя.

Символы секретного ключа отображаются в виде звездочек. После того, как вы начали вводить секретный ключ, отображается кнопка **Показать**. Нажмите на эту кнопку и удерживайте ее необходимое вам время, чтобы просмотреть введенные символы.

Поле доступно, если вы выбрали для авторизации ключ доступа AWS IAM, а не IAM-роль.

Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

- Если вы выбрали Azure, укажите следующие параметры:

  - **Идентификатор приложения в Azure**

    Вы создали этот идентификатор приложения на портале Azure.

    Вы можете указать только один идентификатор приложения в Azure для опроса и других целей. Если необходимо опрашивать другой сегмент Azure, вам нужно сначала удалить первый сегмент в существующем соединении Azure.

  - **Идентификатор подписки Azure**

    Вы создали подписку на портале Azure.

  - **Пароль приложения Azure**

    Вы получили пароль к идентификатору приложения при создании ID приложения в Azure.

    Символы пароля отображаются в виде звездочек. После того, как вы начали вводить пароль, отображается кнопка **Показать**. Нажмите и удерживайте эту кнопку, чтобы просмотреть введенные символы.

    Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

  - **Имя учетной записи хранения Azure**

    Вы создали имя учетной записи хранения Azure для работы с Kaspersky SIEM Cloud.

  - **Ключ доступа хранилища Azure**

    Вы получили пароль (ключ) при создании учетной записи хранения Azure для работы с Kaspersky SIEM Cloud.

    Ключ доступен в разделе "Overview of the Azure storage account" в подразделе "Keys".

    Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

Если вы выбрали Google Cloud, укажите следующие параметры:

- **Электронная почта клиента**

  Электронная почта клиента – это адрес электронной почты, который вы использовали для регистрации вашего проекта в Google Cloud.

- **ID проекта**

  Идентификатор проекта – это идентификатор, полученный при регистрации проекта Google Cloud.

- **Закрытый ключ**

  Закрытый ключ – это последовательность символов, которые вы получили в качестве закрытого ключа при регистрации проекта в Google Cloud. Вы можете скопировать и вставить эту последовательность, чтобы избежать ошибок.

Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

6. Нажмите на кнопку **Настроить расписание опроса**, чтобы изменить параметры по умолчанию.

Соединение сохранится в параметрах приложения.

После первого опроса нового облачного сегмента появится подгруппа в группе администрирования **Управляемые устройства****Cloud**, соответствующая этому сегменту.

Если вы указали неверные учетные данные, то инстансы не будут найдены во время опроса облачного сегмента, а новая подгруппа не будет отображаться в группе **Управляемые устройства****Cloud**.

Удаление соединения для опроса облачных сегментов

Если вам больше не нужно опрашивать какой-либо облачный сегмент, вы можете удалить соединение, соответствующее этому сегменту, из списка доступных. Вы также можете удалить соединение, если, например, права на опрос облачного сегмента перешли к другому пользователю с другими учетными данными.

Чтобы удалить соединение:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Cloud**.
2. В появившемся окне нажмите **Свойства**.
3. В открывшемся окне **Параметры** нажмите на имя сегмента, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.
5. В появившемся окне нажмите на кнопку **ОК**, чтобы подтвердить свой выбор.

Соединение удалено. Устройства в облачном сегменте, соответствующие этому соединению, автоматически удаляются из групп администрирования.

Настройка расписания опроса с помощью Kaspersky Security Center Cloud Console

Опрос облачного сегмента происходит по расписанию. Вы можете задать периодичность, с которой происходит опрос.

На этапе работы мастера настройки для работы в облачном окружении автоматически задается периодичность опроса раз в пять минут. Вы можете изменить это значение в любое время и задать другое расписание. Не рекомендуется производить опрос чаще, чем раз в пять минут, так как это может привести к ошибкам в работе API.

Чтобы настроить расписание опроса облачного сегмента:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Cloud**.

2. В появившемся окне нажмите **Свойства**.

3. В открывшемся окне **Параметры** нажмите на имя сегмента, для которого вы хотите настроить расписание опроса.

   Откроется окно **Параметры облачного сегмента**.

4. В окне **Параметры облачного сегмента** нажмите на кнопку **Настроить расписание опроса**.

   Отобразится окно **Расписание**.

5. В окне **Расписание** укажите следующие параметры:

   - **Запуск по расписанию**

     Варианты расписания опроса:

     - **Каждые N дней**

       Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

       По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

     - **Каждые N минут**

       Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

       По умолчанию опрос запускается каждые пять минут, начиная с текущего системного времени.

     - **По дням недели**

       Опрос выполняется регулярно, в указанные дни недели, в указанное время.

       По умолчанию опрос запускается каждую пятницу в 18:00:00.

     - **Ежемесячно, в указанные дни выбранных недель**

       Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

       По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

   - **Интервал запуска (сут)**

     Укажите значение N (для минут или дней).

   - **Начиная с момента**

     Укажите начало первого опроса.

   - **Запускать пропущенные задачи**

     Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

     Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

     Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

По умолчанию параметр включен.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Расписание опроса для сегмента настроено и сохранено.

Просмотр результатов опроса облачного сегмента с помощью Kaspersky Security Center Cloud Console

Вы можете просмотреть результаты опроса облачного сегмента, то есть просмотреть список облачных устройств, управляемых Сервером администрирования.

Чтобы просмотреть результаты опроса облачного сегмента:

В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Cloud**.

Отображаются облачные сегменты, доступные для опроса.

Просмотр свойств облачных устройств с помощью OSMP Console

Вы можете просмотреть свойства каждого облачного устройства.

Чтобы просмотреть свойства облачного устройства:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
2. Выберите устройство, свойства которого требуется просмотреть.

   В открывшемся окне свойств выберите раздел **Общие**.
3. Если вы хотите просмотреть свойства требуемых облачных устройств, в окне свойств выберите раздел **Система**.

   Свойства отображаются в зависимости от того, к какой облачной платформе принадлежит устройство.

   Для устройств в AWS отображаются следующие свойства:

   - **Устройство обнаружено с помощью API** (значение: **AWS**).
   - **Регион облачного окружения.**
   - **VPC.**
   - **Облачная зона доступности.**
   - **Облачная подсеть.**
   - **Облачная группа размещения** (это устройство отображается, если инстанс принадлежит группе размещения; в противном случае свойство не отображается).

Для устройств в Azure отображаются следующие свойства:

- **Устройство обнаружено с помощью API** (значение: **Microsoft Azure**).
- **Регион облачного окружения.**
- **Облачная подсеть.**

Для устройств в Google Cloud отображаются следующие свойства:

- **Устройство обнаружено с помощью API** (значение: **Google Cloud**).
- **Регион облачного окружения.**
- **VPC.**
- **Облачная зона доступности.**
- **Облачная подсеть.**

Синхронизация с облачным сегментом: настройка правила перемещения

Во время работы мастера настройки для работы в облачном окружении автоматически создается правило Синхронизация с облачным окружением. Правило позволяет автоматически перемещать устройства, найденные при каждом опросе, из группы Нераспределенные устройства в группу Управляемые устройства\Cloud, чтобы устройства были доступны для централизованного управления. По умолчанию правило включено после создания. Вы можете выключить, изменить или применить правило в любое время.

Чтобы изменить свойства правила Синхронизация с облачным окружением и/или применить правило:

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Правила перемещения**.

   Откроется список правил перемещения.

2. В списке правил перемещения выберите **Синхронизация с облачным окружением**.

   Откроется окно свойств правила.

3. При необходимости укажите следующие параметры на вкладке **Условия правила** вкладки **Облачные сегменты**:

   - **Устройство находится в облачном сегменте**

     The rule only applies to devices that are in the selected cloud segment. Otherwise, the rule applies to all devices that have been discovered.

     By default, this option is selected.

   - **Включать дочерние объекты**

     The rule applies to all devices in the selected segment and in all nested cloud subsections. Otherwise, the rule only applies to devices that are in the root segment.

     By default, this option is selected.

- **Перемещать устройства в соответствующие подгруппы**

  If this option is enabled, devices from nested objects are automatically moved to the subgroups that correspond to their structure.

  If this option is disabled, devices from nested objects are automatically moved to the root of the Cloud subgroup without any further branching.

  By default, this option is enabled.

- **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств**

  If this option is enabled, when the structure of the **Managed devices\Cloud** group has no subgroups that will match the section containing the device, Kaspersky SIEM Cloud creates such subgroups. For example, if a new subnet is discovered during device discovery, a new group with the same name will be created under the **Managed devices\Cloud** group.

  If this option is disabled, Kaspersky SIEM Cloud does not create any new subgroups. For example, if a new subnet is discovered during network poll, a new group with the same name will not be created under the **Managed devices\Cloud** group, and the devices that are in that subnet will be moved into the **Managed devices\Cloud** group.

  By default, this option is enabled.

- **Удалять подгруппы, для которых нет соответствия в облачных сегментах**

  If this option is enabled, the application deletes from the Cloud group all the subgroups that do not match any existing cloud objects.

  If this option is disabled, subgroups that do not match any of the existing cloud objects are retained.

  By default, this option is enabled.

Если при работе с мастером настройки для работы в облачном окружении вы включили параметр **Синхронизировать группы администрирования с облачной структурой**, то правило **Синхронизация с облачным окружением** создается с включенными параметрами **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств** и **Удалять подгруппы, для которых нет соответствия в облачных сегментах**.

Если вы не включили параметр **Синхронизировать группы администрирования с облачной структурой**, правило **Синхронизация с облачным окружением** создается с отключенными параметрами (флажки сняты). Если в процессе работы с Kaspersky Security Center Cloud Console вам потребуется, чтобы структура подгрупп группы **Управляемые устройства\Cloud** соответствовала структуре облачных сегментов, включите в свойствах правила параметры **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств** и **Удалять подгруппы, для которых нет соответствия в облачных сегментах** и примените правило.

4. Выберите значение в раскрывающемся списке **Устройство обнаружено с помощью API**:

   - **Нет**. Устройство не обнаруживается с помощью AWS, Azure или Google API, то есть оно либо находится вне облачного окружения, либо находится в облачном окружении, но по каким-то причинам недоступно для поиска с помощью API.

   - **AWS**. Устройство обнаружено с использованием AWS API, то есть устройство находится в облачном окружении AWS.

   - **Azure**. Устройство обнаружено с использованием Azure API, то есть устройство находится в облачном окружении Azure.

- **Google Cloud**. Устройство обнаружено с использованием Google API, то есть устройство находится в облачном окружении Google Cloud.
- Не задано. Критерий не может быть применен.

5. При необходимости настройте другие свойства правила в других разделах.

Правило перемещения настроено.

Удаленная установка приложений на виртуальные машины Azure

У вас должна быть действующая лицензия для установки приложений на виртуальные машины Microsoft Azure.

Kaspersky Security Center Cloud Console поддерживает следующие сценарии:

- Клиентское устройство обнаружено с помощью Azure API; установка также выполняется средствами API. Использование Azure API означает, что вы можете установить только следующие приложения:
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows
- Клиентское устройство обнаруживается с помощью Azure API; установка выполняется с помощью точки распространения или, если точки распространения нет, вручную с использованием автономных инсталляционных пакетов. Таким образом вы можете установить любое приложение, поддерживаемое Kaspersky Security Center Cloud Console.

Чтобы создать задачу удаленной установки приложения на виртуальные машины Azure:

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. Следуйте далее указаниям мастера.
   a. Выберите тип задачи **Удаленная установка приложения**.
   b. На странице **Инсталляционные пакеты** выберите **Удаленная установка с помощью Microsoft Azure API**.
   c. При выборе учетной записи для доступа к устройствам используйте существующую учетную запись Azure или нажмите на кнопку **Добавить** и введите учетные данные своей учетной записи Azure:
      - **ИД приложения в Azure**

        Введите любое имя для учетных данных, которые вы указываете. Это имя отображается в списке учетных записей для запуска задачи.
      - **Идентификатор приложения в Azure**

        Вы создали этот идентификатор приложения на портале Azure.

Вы можете указать только один идентификатор приложения в Azure для опроса и других целей. Если необходимо опрашивать другой сегмент Azure, вам нужно сначала удалить первый сегмент в существующем соединении Azure.

- **Пароль приложения Azure**

  Вы получили пароль к идентификатору приложения при создании ID приложения в Azure.

  Символы пароля отображаются в виде звездочек. После того, как вы начали вводить пароль, отображается кнопка **Показать**. Нажмите и удерживайте эту кнопку, чтобы просмотреть введенные символы.

d. Выберите требуемые устройства из группы **Управляемые устройства****Cloud**.

После завершения работы мастера, задача удаленной установки приложения появится в списке задач.

Настройка компонентов Kaspersky SIEM Cloud

Настройка параметров Ядра Kaspersky SIEM Cloud

Чтобы настроить параметры Ядра Kaspersky SIEM Cloud:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В блоке **Другое** нажмите **Общее**.

   Откроется окно **Общее**.

3. В блоке **Параметры ядра** укажите значение следующих параметров:

   - В раскрывающемся списке **День начала недели** выберите первый день недели, который будет использоваться во всем экземпляре Kaspersky SIEM Cloud. Выбранное значение применяется при выборе периодов и указании временных интервалов во всех разделах Kaspersky SIEM Cloud. По умолчанию выбрано значение **Понедельник**. Изменять значение параметра может только пользователь с ролью Главный администратор. Выбранное значение сохраняется в параметрах Ядра Kaspersky SIEM Cloud.

   - В раскрывающемся списке **Локализация ресурсов KUMA** выберите язык локализации ресурсов Kaspersky SIEM Cloud, импортируемых из репозитория. По умолчанию используется английский язык. При изменении параметра только новые ресурсы Kaspersky SIEM Cloud будут импортироваться с выбранным языком. Если до этого вы импортировали ресурсы на другом языке, эти ресурсы останутся без изменения. Чтобы поменять язык уже импортированных ресурсов, вам нужно импортировать их из репозитория заново.

     Параметр **Локализация ресурсов KUMA** не зависит от параметра языка интерфейса Kaspersky SIEM Cloud. Вы можете выбрать разные языки локализации в этих параметрах. В таком случае, например, язык текстов в таблице ресурсов может отличаться от языка локализации интерфейса.

     Параметр **Локализация ресурсов KUMA** не влияет на ресурсы, созданные вручную.

   - При необходимости нажмите на кнопку **Перевыпустить**, чтобы перевыпустить сертификат AI-сервиса и внутренний CA-сертификат.

     > После перевыпуска сертификата AI-сервиса необходимо вручную перезапустить все сервисы. Для применения нового сертификата AI-сервиса требуется перезапуск ядра Kaspersky SIEM Cloud.

4. Если вы не хотите использовать самоподписанный сертификат Kaspersky SIEM Cloud, в блоке **Внешняя TLS-пара** загрузите сертификат и ключ для TLS-пары.

   Нажав на кнопку **Обновить сертификат**, вы можете обновить сертификат для TLS-пары.

5. В блоке **Свойства ядра** укажите значение следующих параметров:

- В поле **Тег активации** укажите применимый тег.
- В поле **Максимальное число одновременно запускаемых сервисов** укажите количество сервисов, которые Kaspersky SIEM Cloud может запускать одновременно.

  По умолчанию установлено значение 10.

  > Слишком большое количество одновременно запускаемых сервисов может привести к замедлению обработки данных Kaspersky SIEM Cloud.

- В поле **Срок действия исключения для создания алерта, часы** укажите период хранения исключений для корреляционных правил в часах. Вы можете указать значение от 1 до 24*365 включительно.

  По умолчанию установлено значение 72 часа.

- В поле **Таймаут отправки событий через служебную точку назначения Core, секунды** укажите время ожидания установки соединения с сервисом при отправке событий. Вы можете указать любое время ожидания больше 0 секунд.

  По умолчанию установлено значение 15 секунд.

- В поле **Час суток, в который Core имеет право выполнять задачи по самообслуживанию** укажите время (в формате UTC), когда ядро может осуществлять операции по самостоятельному обслуживанию. Ядро KUMA выполняет такие операции ежедневно. Вы можете указать значение от 0 до 23 включительно.

  > Рекомендуется проводить операции по обслуживанию Ядра KUMA в ночное время, когда пользователи не используют функциональные возможности Ядра KUMA.

  По умолчанию установлено значение 1 (время в формате UTC).

- В поле **Срок хранения истории ресурсов, дни** укажите время хранения истории изменения ресурсов в днях. Вы можете установить любое значение больше или равное 0.

  По умолчанию указано значение 12 дней.

- В поле **Время ожидания запроса кластеров из UI, секунды** укажите время, в течение которого веб-клиент Kaspersky SIEM Cloud ждет ответ на запрос списка хранилищ. Вы можете установить любое значение больше 0.

  По умолчанию указано значение 30 секунд.

- В поле **Время ожидания проверки работоспособности узлов хранилища, секунды** укажите время ожидания ответа на запрос о проверке доступности определенных узлов хранилища. Вы можете установить любое значение больше 0.

  По умолчанию указано значение 30 секунд.

6. Нажмите **Сохранить**.

Сбор и обогащение событий

В этом разделе описано, как настроить получение, обработку и обогащение событий для дальнейшего анализа.

Подключение источников событий

В этом разделе представлена информация о настройке получения событий из разных источников.

Kaspersky

В этом разделе описана настройка получения событий от продуктов Kaspersky, используемых для мониторинга безопасности и интеграции с Kaspersky SIEM Cloud.

Kaspersky Security Center (Сервер администрирования)

Настройка получения и передачи событий от Сервера администрирования Kaspersky Security Center в Kaspersky SIEM Cloud состоит из следующих этапов:

1. Настройка передачи событий Kaspersky Security Center

Kaspersky Security Center позволяет настроить параметры экспорта событий в SIEM-систему в формате CEF.

> Функция экспорта событий Kaspersky Security Center в SIEM-системы в формате CEF доступна при наличии лицензии Kaspersky Endpoint Security для бизнеса Расширенный или выше.

1. В дереве консоли Kaspersky Security Center выберите узел **Сервер администрирования**.
2. В рабочей области узла выберите вкладку **События**.
3. Перейдите по ссылке **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите **Настроить экспорт в SIEM-систему**.

   Откроется окно **Свойства: События**. По умолчанию откроется раздел **Экспорт событий**.
4. В разделе **Экспорт событий** установите флажок **Автоматически экспортировать события в базу SIEM-системы**.
5. В раскрывающемся списке **SIEM-система** выберите **ArcSight (CEF-формат)**.

6. Укажите адрес сервера SIEM-системы Kaspersky SIEM Cloud и порт для подключения к серверу в соответствующих полях. В качестве протокола выберите **TCP/IP**.

   Вы можете нажать на кнопку **Экспортировать архив** и указать дату, начиная с которой уже созданные события Kaspersky SIEM Cloud будут экспортироваться в базу SIEM-системы. По умолчанию Kaspersky Security Center экспортирует события с текущей даты.

7. Нажмите на кнопку **OK**.

Сервер администрирования Kaspersky Security Center будет автоматически экспортировать все события в Kaspersky SIEM Cloud.

❷ Настройка коллектора Kaspersky SIEM Cloud для получения событий Kaspersky Security Center

После завершения настройки экспорта событий от Сервера администрирования Kaspersky Security Center в формате CEF вам нужно настроить коллектор в веб-интерфейсе Kaspersky SIEM Cloud.

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Коллекторы**.

2. В списке коллекторов найдите коллектор с нормализатором **[OOTB] KSC** и нажмите на него, чтобы открыть для редактирования.

3. На шаге **Транспорт** в поле **URL** укажите порт, по которому коллектор будет получать события Kaspersky Security Center.

   Порт должен совпадать с портом сервера SIEM-системы Kaspersky SIEM Cloud.

4. На шаге **Парсинг событий** проверьте, что выбран нормализатор **[OOTB] KSC**.

5. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:

   - **Хранилище**. Для отправки обработанных событий в хранилище.
   - **Коррелятор**. Для отправки обработанных событий в коррелятор.

   Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

6. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

7. Скопируйте появившуюся команду для установки коллектора Kaspersky SIEM Cloud.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения настройки коллектора для сбора событий Kaspersky Security Center в формате CEF требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Проверка поступления событий Kaspersky Security Center в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что экспорт событий из Сервера администрирования Kaspersky Security Center в SIEM-систему Kaspersky SIEM Cloud выполнен правильно, выполнив поиск связанных событий.

Чтобы отобразить события Kaspersky Security Center в таблице, введите поисковое выражение.

Пример

```
SELECT
    Timestamp,
    Severity,
    Message
FROM events
WHERE DeviceProduct = 'KSC'
ORDER BY Timestamp DESC
LIMIT 250
```

Kaspersky Security Center (MS SQL)

Настройка получения информации о событиях Kaspersky Security Center из базы данных MS SQL (далее MS SQL) в Kaspersky SIEM Cloud состоит из следующих этапов:

1 Создание учетной записи в MS SQL

Для получения событий Kaspersky Security Center из MS SQL требуется учетная запись, которая имеет права, необходимые для подключения и работы с базой данных.

1. Войдите на сервер с установленной MS SQL для Kaspersky Security Center.
2. С помощью **SQL Server Management Studio** подключитесь к MS SQL под учетной записью с правами администратора.
3. В панели **Object Explorer** раскройте раздел **Security**.
4. Нажмите правой кнопкой мыши на папку **Logins** и в контекстном меню выберите **New Login**.

   Откроется окно **Login - New**.
5. На вкладке **General** нажмите на кнопку **Search** рядом с полем **Login name**.

   Откроется окно **Select User or Group**.
6. В поле **Enter the object name to select (examples)** укажите имя объекта и нажмите **OK**.

   Окно **Select User or Group** закроется.
7. В окне **Login - New** на вкладке **General** выберите **Windows authentication**.
8. В поле **Default database** выберите базу данных Kaspersky Security Center.

   По умолчанию имя базы данных – `Kaspersky Security Center: KAV`.
9. На вкладке **User Mapping** настройте права для учетной записи:

   a. В разделе **Users mapped to this login** выберите базу данных Kaspersky Security Center.

   b. В разделе **Database role membership for** установите флажки возле прав **db_datareader** и **public**.
10. На вкладке **Status** настройте права для подключения учетной записи к базе данных:

    - В разделе **Permission to connect to database engine** выберите **Grant**.
    - В разделе **Login** выберите **Enabled**.

11. Нажмите **OK**.

    Окно **Login - New** закроется.

После создания учетной записи, необходимо проверить настроенные права. Для этого вам нужно запустить **SQL Server Management Studio** под созданной учетной записью, а затем перейти в любую таблицу MS SQL и сделать выборку по этой таблице.

❷ Настройка службы SQL Server Browser

После создания учетной записи в MS SQL требуется настроить службу SQL Server Browser.

1. Откройте **SQL Server Configuration Manager**.
2. В левой панели выберите **SQL Server Services**.

   Откроется список служб.
3. Откройте свойства службы **SQL Server Browser** одним из следующих способов:

   - Дважды нажмите на название службы **SQL Server Browser**.
   - Нажмите правой кнопкой мыши на название службы **SQL Server Browser** и в контекстном меню выберите **Properties**.
4. В открывшемся окне **SQL Server Browser Properties** выберите вкладку **Service**.
5. В поле **Start Mode** выберите **Automatic**.
6. Выберите вкладку **Log On** и нажмите на кнопку **Start**.

   Автоматический запуск службы **SQL Server Browser** включен.
7. Включите и настройте протокол **TCP/IP**, выполнив следующие действия:

   a. В левой панели раскройте раздел **SQL Server Network Configuration** и выберите подраздел **Protocols for <Имя SQL-сервера>**.

   b. Нажмите правой кнопкой мыши на протокол **TCP/IP** и в контекстом меню выберите **Enable**.

   c. В появившемся окне **Warning** нажмите **OK**.

   d. Откройте свойства протокола **TCP/IP** одним из следующих способов:

      - Дважды нажмите на протокол **TCP/IP**.
      - Нажмите правой кнопкой мыши на протокол **TCP/IP** и в контекстном меню выберите **Properties**.

   e. Выберите вкладку **IP Addresses**, а затем в разделе **IPALL** в поле **TCP Port** укажите порт 1433.

   f. Нажмите на кнопку **Apply**, чтобы сохранить внесенные изменения.

   g. Нажмите на кнопку **OK**, чтобы закрыть окно.

8. Перезагрузите службу **SQL Server (<Имя SQL-сервера>)**, выполнив следующие действия:

   a. В левой панели выберите **SQL Server Services**.

   b. В списке служб справа нажмите правой кнопкой мыши на службу **SQL Server (<Имя SQL-сервера>)** и в контекстном меню выберите **Restart**.

9. Для параметра **Брандмауэр защитника Windows в режиме повышенной безопасности** разрешите на сервере входящие подключения по порту TCP 1433.

3 Создание секрета

После создания и настройки учетной записи в MS SQL требуется добавить секрет в веб-консоли. Этот ресурс используется для хранения учетных данных для подключения к MS SQL.

1. В веб-консоли откройте раздел **Мониторинг** → **Ресурсы и сервисы** → **Секреты**.

   Отобразится список доступных секретов.

2. Нажмите на кнопку **Добавить секрет**, чтобы создать новый секрет.

   Откроется окно секрета.

3. Введите данные секрета:

   a. В поле **Название** выберите имя для добавляемого секрета.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать создаваемый ресурс.

   c. В раскрывающемся списке **Тип** выберите **urls**.

   d. В поле **URL** укажите строку вида:

   ```
   sqlserver://[<domain>%5C]<username>:<password>@<server>:1433/<database_name>
   ```

   где:

   - `domain` – имя домена.
   - `%5C` – разделитель домена и пользователя. Представляет собой знак "\" в URL-формате.
   - `username` – имя созданной учетной записи MS SQL.
   - `password` – пароль созданной учетной записи MS SQL.
   - `server` – имя или IP-адрес сервера с базой данных MS SQL, установленной для Kaspersky Security Center.
   - `database_name` – имя базы данных Kaspersky Security Center. Имя по умолчанию: KAV.

   Пример

   ```
   sqlserver://test.local%5Cuser:password123@10.0.0.1:1433/KAV
   ```

Если в пароле учетной записи MS SQL используются специальные символы (@ # $ % & * ! + = [ ] : ' , ? / \ ` ( ) ;), переведите их в формат URL.

4. Нажмите **Сохранить**.

Для безопасности после сохранения секрета строка, указанная в поле **URL**, скрывается.

❹ Настройка коннектора

Для подключения Kaspersky SIEM Cloud к MS SQL требуется настроить коннектор.

1. В веб-интерфейсе откройте раздел **Мониторинг** → **Ресурсы и сервисы** → **Коннекторы**.
2. В списке коннекторов справа найдите коннектор **[OOTB] KSC SQL** и откройте его для редактирования.

   Если коннектор недоступен для редактирования, скопируйте его и откройте для редактирования копию коннектора. Если коннектор **[OOTB] KSC SQL** отсутствует, обратитесь к системному администратору.

3. На вкладке **Основные параметры** в раскрывающихся списках **URL** выберите секрет, созданный для подключения к MS SQL.
4. Нажмите **Сохранить**.

❺ Создание коллектора Kaspersky SIEM Cloud для получения событий Kaspersky Security Center из MS SQL

При создании коллектора в веб-консоли на шаге **Транспорт** выберите коннектор **[OOTB] KSC SQL**, а на шаге **Парсинг событий** выберите нормализатор **[OOTB] KSC from SQL**.

❻ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для получения событий Kaspersky Security Center из MS SQL требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❼ Проверка поступления событий из MS SQL в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка поступления событий из MS SQL выполнена правильно, выполнив поиск связанных событий.

Kaspersky Web Traffic Security

Вы можете настроить получение событий из системы анализа и фильтрации веб-трафика Kaspersky Web Traffic Security (KWTS) в Kaspersky SIEM Cloud.

Настройка получения событий состоит из следующих этапов:

❶ Настройка передачи событий KWTS в Kaspersky SIEM Cloud

В зависимости от используемой версии KWTS вы можете использовать одну из следующих инструкций:

[Для KWTS 6.2](#)

Для KWTS 6.1

Чтобы настроить передачу событий KWTS в Kaspersky SIEM Cloud:

1. Подключитесь к серверу KWTS по протоколу SSH под учетной записью root.
2. Перед внесением изменений создайте резервные копии следующих файлов:
   - `/opt/kaspersky/kwts/share/templates/core_settings/event_logger.json.template`
   - `/etc/rsyslog.conf`
3. Убедитесь, что параметры конфигурационного файла `/opt/kaspersky/kwts/share/templates/core_settings/event_logger.json.template` имеют следующие значения, при необходимости внесите изменения:

```
"siemSettings":
{
"enabled": true,
"facility": "Local5",
"logLevel": "Info",
"formatting":
{
```

4. Сохраните внесенные изменения.
5. Для отправки событий по протоколу UDP внесите следующие изменения в конфигурационный файл `/etc/rsyslog.conf`:

```
$WorkDirectory /var/lib/rsyslog
$ActionQueueFileName ForwardToSIEM
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
local5.* @<<Kaspersky SIEM Cloud collector IP address>:<Collector port>>
```

   Если вы хотите отправлять события по протоколу TCP, последняя строчка должна выглядеть следующим образом:

```
local5.* @@<<Kaspersky SIEM Cloud collector IP address>:<Collector port>>
```

6. Сохраните внесенные изменения
7. Перезапустите сервис rsyslog с помощью следующей команды:

```
sudo systemctl restart rsyslog.service
```

8. Перейдите в веб-интерфейс KWTS на вкладку **Параметры** – **Syslog** и включите опцию **Записывать информацию о профиле трафика**.

9. Нажмите **Сохранить**.

❷ Настройка экспорта событий в формате CEF

Если вы настраиваете получение событий из KWTS 6.2, следуйте инструкции в документации KWTS 6.2, чтобы включить экспорт событий.

❸ Создание коллектора Kaspersky SIEM Cloud для получения событий KWTS

Для получения событий KWTS при создании коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] KWTS**.

❹ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре для получения событий KWTS

После завершения создания и настройки коллектора для сбора событий Kaspersky Web Traffic Security требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❺ Проверка поступления событий KWTS в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка передачи событий KWTS выполнена правильно, выполнив поиск связанных событий.

Kaspersky Linux Mail Server

Настройка получения событий из системы анализа и фильтрации почтового трафика Kaspersky Linux Mail Server (KLMS) в Kaspersky SIEM Cloud состоит из следующих этапов:

❶ Настройка передачи событий из KLMS в Kaspersky SIEM Cloud

В зависимости от используемой версии KLMS вы можете использовать одну из следующих инструкций:

Для KLMS 10 в Kaspersky SIEM Cloud (документация для KLMS 10 доступна только на русском языке)

Для KLMS 8 в Kaspersky SIEM Cloud

Чтобы настроить передачу событий KLMS в Kaspersky SIEM Cloud:

1. Подключитесь к серверу KLMS по протоколу SSH и перейдите в меню **Technical Support Mode**.

2. С помощью утилиты klms-control выгрузите настройки в файл `settings.xml`:

```
sudo /opt/kaspersky/klms/bin/klms-control --get-settings EventLogger -n -f /tmp/settings.xml
```

3. Убедитесь, что параметры файла `/tmp/settings.xml` имеют следующие значения, при необходимости внесите изменения:

```
<siemSettings>
        <enabled>1</enabled>
        <facility>Local1</facility>
...
</siemSettings>
```

4. Примените настройки с помощью следующей команды:

```
sudo /opt/kaspersky/klms/bin/klms-control --set-settings EventLogger -n -f /tmp/settings.xml
```

5. Для отправки событий по протоколу UDP внесите следующие изменения в конфигурационный файл `/etc/rsyslog.conf`.

```
$WorkDirectory /var/lib/rsyslog
$ActionQueueFileName ForwardToSIEM
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
local1.* @<<collector_IP>:<collector_port>>
```

Если вы хотите отправлять события по протоколу TCP, последняя строчка должна выглядеть следующим образом:

```
local1.* @@<<collector_IP>:<collector_port>>
```

где:

- <collector_IP> — IP-адрес коллектора.
- <collector_port> — порт коллектора.

6. Сохраните внесенные изменения.

7. Перезапустите сервис rsyslog с помощью следующей команды:

```
sudo systemctl restart rsyslog.service
```

❷ Создание коллектора Kaspersky SIEM Cloud для получения событий KLMS

При создании коллектора в веб-консоли на шаге **Парсинг событий** выберите нормализатор **[OOTB] KLMS syslog CEF**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Kaspersky Linux Mail Server требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

4 Проверка поступления событий KLMS в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий KLMS выполнена правильно, выполнив поиск связанных событий.

Kaspersky Secure Mail Gateway

Настройка получения событий из системы анализа и фильтрации почтового трафика Kaspersky Secure Mail Gateway (KSMG) в Kaspersky SIEM Cloud состоит из следующих этапов:

1 Настройка передачи событий KSMG в Kaspersky SIEM Cloud

KSMG может публиковать события, происходящие во время работы приложения, в Kaspersky SIEM Cloud по протоколу Syslog.

Информация о каждом событии приложения передается как отдельное syslog-сообщение формата CEF. По умолчанию экспорт CEF-сообщений в приложении выключен. Вы можете настроить публикацию событий в SIEM-систему и включить экспорт событий.

2 Создание коллектора Kaspersky SIEM Cloud для получения событий KSMG

При создании коллектора в веб-консоли на шаге **Парсинг событий** выберите нормализатор **[OOTB] KSMG**.

3 Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Kaspersky Secure Mail Gateway требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

4 Проверка поступления событий KSMG в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий KSMG выполнена правильно, выполнив поиск связанных событий.

Kaspersky Industrial CyberSecurity for Networks

Настройка получения событий из программы Kaspersky Industrial CyberSecurity for Networks (KICS for Networks) версии 4.2 в Kaspersky SIEM Cloud состоит из следующих этапов:

1 Создание коннектора KICS for Networks для передачи событий в Kaspersky SIEM Cloud

1. Войдите в веб-интерфейс KICS for Networks под учетной записью администратора.
2. Перейдите в раздел **Параметры** → **Коннекторы**.
3. Нажмите на кнопку **Добавить коннектор**.

4. Укажите следующие параметры:

   a. В раскрывающемся списке **Тип коннектора** выберите значение **SIEM**.

   b. В поле **Имя коннектора** укажите имя для коннектора.

   c. В поле **Адрес Сервера** введите IP-адрес Сервера KICS for Networks.

   d. В раскрывающемся списке **Узел размещения коннектора** выберите узел, на котором вы устанавливаете коннектор.

      Вы можете указать любое имя.

   e. В поле **Имя пользователя** укажите имя пользователя, под которым Kaspersky SIEM Cloud будет подключаться к программе через коннектор. Требуется указать имя одного из пользователей KICS for Networks.

   f. В поле **Адрес-SIEM сервера** введите IP-адрес сервера коллектора Kaspersky SIEM Cloud.

   g. В поле **Номер порта** введите номер порта коллектора Kaspersky SIEM Cloud.

   h. В раскрывающемся списке **Транспортный протокол** выберите одно из следующих значений: **TCP** или **UDP**.

   i. Установите флажок **Разрешить отправку записей аудита**.

   j. Установите флажок **Разрешить отправку записей программы**.

5. Нажмите на кнопку **Сохранить**.

Коннектор будет создан и отобразится в таблице коннекторов KICS for Networks со статусом **Работает**.

❷ Настройка передачи событий KICS for Networks в Kaspersky SIEM Cloud

Чтобы события безопасности KICS for Networks передавались в Kaspersky SIEM Cloud:

1. Войдите в веб-интерфейс KICS for Networks под учетной записью администратора.
2. Перейдите в раздел **Параметры** → **Типы событий**.
3. Установите флажки для типов событий, которые вы хотите передавать в Kaspersky SIEM Cloud.
4. Нажмите на кнопку **Выбрать коннекторы**.
5. В открывшемся окне выберите коннектор, созданный для передачи событий в Kaspersky SIEM Cloud.
6. Нажмите на кнопку **Ok**.

Выбранные типы событий будут передаваться в Kaspersky SIEM Cloud. В таблице **Типы событий** эти типы событий отмечаются флажком в столбце с названием коннектора.

❸ Создание коллектора Kaspersky SIEM Cloud для получения событий KICS for Networks

При создании коллектора в веб-консоли вам нужно выполнить следующие требования:

1. На шаге **Транспорт** требуется выбрать тип транспортного протокола и номер порта, соответствующие выбранным при создании коннектора в KICS for Networks.

2. На шаге **Парсинг событий** требуется выбрать нормализатор **[OOTB] KICS4Net v3.x**.

3. На шаге **Маршрутизация** нужно убедиться, что в набор ресурсов коллектора добавлены следующие точки назначения:

   - **storage** – используется для передачи данных в хранилище.
   - **correlator** – используется для передачи данных в коррелятор.

   Если точки назначения не добавлены в коллектор, вам нужно создать их.

4. На последнем шаге мастера в нижней части окна отобразится команда, с помощью которой вы можете установить сервис на сервер, предназначенный для получения событий. Вам нужно скопировать эту команду и использовать при установке второй части коллектора.

❹ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий KICS for Networks требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❺ Проверка поступления событий KICS for Networks в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка передачи событий KICS for Networks выполнена правильно, выполнив поиск связанных событий.

Kaspersky Anti Targeted Attack Platform

Настройка получения событий программы Kaspersky Anti Targeted Attack Platform в Kaspersky SIEM Cloud состоит из следующих этапов:

❶ Настройка передачи событий Kaspersky Anti Targeted Attack Platform

1. В браузере на любом компьютере, на котором разрешен доступ к серверу Central Node, введите IP-адрес сервера с компонентом Central Node.

   Откроется окно ввода учетных данных пользователя Kaspersky Anti Targeted Attack Platform.

2. В окне ввода учетных данных пользователя установите флажок **Локальный администратор** и введите данные Администратора.

3. Перейдите в раздел **Параметры** → **SIEM-система**.

4. Укажите следующие параметры:

   a. Установите флажки **Журнал активности** и **Обнаружения**.

   b. В поле **Хост/IP** введите IP-адрес или имя хоста коллектора Kaspersky SIEM Cloud.

   c. В поле **Порт** укажите номер порта подключения к коллектору Kaspersky SIEM Cloud.

   d. В поле **Протокол** выберите из списка **TCP** или **UDP**.

   e. В поле **ID хоста** укажите идентификатор хоста сервера, который будет указан в журнале SIEM-систем как источник обнаружения.

   f. В поле **Периодичность сигнала** введите интервал отправки сообщений: от 1 до 59 минут.

   g. При необходимости включите TLS-шифрование.

5. Нажмите на кнопку **Применить**.

Передача событий Kaspersky Anti Targeted Attack Platform в Kaspersky SIEM Cloud настроена

❷ Создание коллектора Kaspersky SIEM Cloud для получения событий Kaspersky Anti Targeted Attack Platform

При создании коллектора в веб-консоли убедитесь, что номер порта и тип коннектора соответствуют порту и коннектору, которые вы указали при настройке передачи событий Kaspersky Anti Targeted Attack Platform в Kaspersky SIEM Cloud. Для получения событий Kaspersky Anti Targeted Attack Platform с помощью Syslog на шаге **Парсинг событий** выберите нормализатор **[OOTB] KATA**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Kaspersky Anti Targeted Attack Platform требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Проверка поступления событий Kaspersky Anti Targeted Attack Platform в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий Kaspersky Anti Targeted Attack Platform выполнена правильно, выполнив поиск связанных событий. События Kaspersky Anti Targeted Attack Platform отображаются в таблице с результатами поиска как KATA.

Kaspersky Endpoint Security for Windows

В Kaspersky Endpoint Security for Windows, начиная с версии 12.6, есть возможность отправлять события из журналов Windows в коллектор Kaspersky SIEM Cloud. Это позволяет получать в Kaspersky SIEM Cloud события из журналов Windows со всех хостов, на которых установлен Kaspersky Endpoint Security for Windows версии 12.6 и выше, без установки агентов Kaspersky SIEM Cloud на эти хосты.

Kaspersky Endpoint Security for Windows версии 12.6–12.10 поддерживает ограниченный набор EventID продуктов компании Microsoft.
В версиях Kaspersky Endpoint Security for Windows 12.6-12.12 схожие по параметрам события фильтруются и отправляется первое из них, а последующие аналогичные события не передаются. При массовом возникновении однотипных событий некоторые из них будут отправлены, для этого может потребоваться появление порядка сотен и тысяч схожих событий. При этом отличающееся событие, например, при входе другого пользователя, будет отправлено. Логика фильтрации определена экспертами "Лаборатории Касперского" и позволяет снизить объем передаваемых событий без потери данных, необходимых для обнаружения атак.

Для активации функциональности требуется:

- иметь действующую лицензию Kaspersky SIEM Cloud.
- использовать Kaspersky Security Center 14.2 и выше.
- использовать Kaspersky Endpoint Security for Windows 12.6 или выше.

Настройка получения событий состоит из следующих этапов:

1. Импорт нормализатора в Kaspersky SIEM Cloud

В Kaspersky SIEM Cloud должно быть настроено получение обновлений через серверы обновлений "Лаборатории Касперского".

В разделе **Ресурсы и сервисы** нажмите **Импортировать ресурсы** и выберите **[OOTB] Microsoft Products via KES WIN** в списке доступных к установке нормализаторов.

2. Создание коллектора Kaspersky SIEM Cloud для получения событий Windows

Вам нужно создать коллектор для получения событий Windows. В зависимости от используемой версии Kaspersky Endpoint Security for Windows выполните следующие действия:

- Если вы используете Kaspersky Endpoint Security for Windows версии 12.6–12.10, на шаге **Транспорт** выберите **TCP** или **UDP** и укажите номер порта, который будет прослушивать коллектор. На шаге **Парсинг событий** выберите нормализатор **[OOTB] Microsoft Products via KES WIN** и на шаге **Фильтрация событий** выберите фильтр **[OOTB] Microsoft Products via KES WIN - Event filter for collector**.
- Если вы используете Kaspersky Endpoint Security for Windows версии 12.11 и выше, на шаге **Транспорт** выберите **TCP** или **UDP** и укажите номер порта, который будет прослушивать коллектор. На шаге **Парсинг событий** выберите нормализатор **[OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1**.

❸ Запрос ключа в Службе технической поддержки

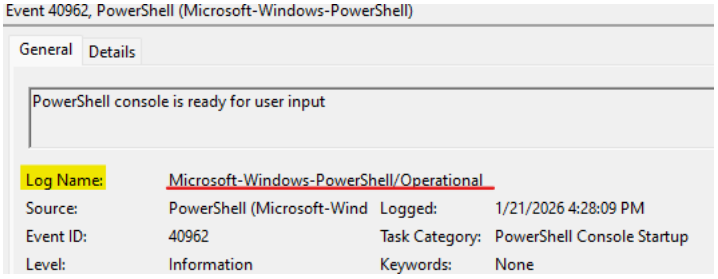
Если в вашей лицензии не было ключа активации функционала отправки журналов Windows в коллектор Kaspersky SIEM Cloud, направьте в Службу технической поддержки письмо следующего содержания: "У нас приобретена лицензия Kaspersky SIEM Cloud и используется Kaspersky Endpoint Security for Windows версии 12.6. Мы планируем активировать функционал отправки журналов Windows в коллектор Kaspersky SIEM Cloud. Просим предоставить файл ключа для активации соответствующего функционала". Новым пользователям Kaspersky SIEM Cloud не требуется писать запрос в Службу технической поддержки, поскольку новым пользователям будет предоставлено два ключа с лицензиями для Kaspersky SIEM Cloud и для активации функциональности Kaspersky Endpoint Security for Windows.

В ответ на письмо вам будет предоставлен файл ключа.

❹ Настройка на стороне Kaspersky Security Center и Kaspersky Endpoint Security for Windows

Файл ключа, активирующий функционал отправки событий Windows в коллекторы Kaspersky SIEM Cloud, необходимо импортировать в Kaspersky Security Center и распространить по конечным устройствам Kaspersky Endpoint Security в соответствии с инструкцией. Также необходимо в политике Kaspersky Endpoint Security добавить адреса серверов Kaspersky SIEM Cloud и настроить сетевые параметры подключения.

Для Kaspersky Endpoint Security for Windows версии 12.11 и выше при добавлении пользовательских журналов в политике Kaspersky Endpoint Security нужно указывать имя журнала в соответствии со значением поля **Log name** в событиях этого журнала (например для журнала Sysmon необходимо указать Microsoft-Windows-Sysmon/Operational).



Поле **Log Name** в событии пользовательского журнала Windows

❺ Проверка поступления событий Windows в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий Windows выполнена правильно, выполнив поиск связанных событий.

Перечень событий продуктов Microsoft, которые Kaspersky Endpoint Security for Windows версии 12.6–12.10 передает в Kaspersky SIEM Cloud, приведен в таблице ниже.

Журнал событий	Идентификатор события
System	12 13 7040 7045 42 104 107 109 1074 6005 6006 7034 7036 8003

Журнал событий	Идентификатор события
Security	1102 4614 4649 4696 4698 4704 4706 4713 4715 4717 4720 4723 4724 4725 4726 4727 4728 4729 4738 4739 4740 4741 4742 4756 4757 4765 4766 4767 4768 4769 4770 4771 4775 4776 4778 4780 4781 4794 4817 4876 4877 4882 4885 4886 4887 4890 4891 4898 4904 4905 4928 4950 4964 5136 5137 5138 5139 5141 5142 5143 5144 5155 5376 5377 5632 5888 5890 6416 4622 4648 4672 4697 4702 4719 4732 4733

Журнал событий	Идентификатор события
	4798 4946 4947 4948 4949 5145 4616 4625 4663 4624 4799 5140 1008 1105 2722 4615 4618 4626 4627 4634 4647 4653 4654 4656 4657 4658 4659 4660 4661 4664 4666 4667 4670 4673 4674 4688 4689 4690 4691 4692 4693 4694 4695 4699 4700 4701 4703 4705 4707 4714 4716 4718 4730 4731 4734 4737 4743 4744 4745 4746 4747 4748 4749 4750 4751 4752 4753 4754 4755 4758 4759 4760 4761 4762 4763 4764

Журнал событий	Идентификатор события
	4772
	4773
	4774
	4777
	4779
	4782
	4783
	4784
	4785
	4786
	4787
	4788
	4789
	4790
	4791
	4792
	4793
	4797
	4800
	4801
	4802
	4803
	4818
	4819
	4820
	4821
	4822
	4823
	4824
	4825
	4826
	4865
	4866
	4867
	4868
	4869
	4870
	4871
	4872
	4873
	4874
	4875
	4883
	4884
	4888
	4892
	4893
	4896
	4906
	4907
	4908
	4911
	4912
	4913
	4929
	4930
	4931
	4932
	4933
	4935
	4944
	4945
	4951
	4953
	4956
	4957
	4958
	4981
	4982
	4983
	4984
	4985
	5024
	5031
	5033
	5039

Журнал событий	Идентификатор события
	5049 5051 5056 5057 5058 5059 5060 5061 5063 5064 5065 5066 5067 5068 5069 5070 5071 5122 5123 5146 5147 5152 5153 5154 5156 5157 5158 5159 5168 5378 5379 5380 5381 5382 5447 5448 5451 5452 5459 5461 5472 5474 5477 5478 5483 5484 5633 6144 6145 6272 6273 6274 6276 6278 6279 6280 6281 6410 6419 6420 6421 6422 6423 6424 6889

Журнал событий	Идентификатор события
PowerShell	4100 4103 4104 4105 4106 8193 8194 8197 24577 24595 24596 24597 24598 24599 53249 53250 53504
MS SQL Server	615 919 958 1945 2007 2812 3406 3407 3421 3454 5084 5579 5701 5703 6253 8128 9013 9666 15268 15457 17104 17110 17111 17125 17137 17152 17164 17176 17177 17199 17201 17550 17551 17561 17663 18264 18265 18456 18488 18496 19030 19031 19032 26022 26037 26048 26067 33090 49903 49904

Журнал событий	Идентификатор события
Microsoft Defender	1006 1015 1116 1117 1000 1001 2000 5000 5001 5002 5004 5007 5010 5012
Terminal Server	1149 21 22 24 25 39 40
Microsoft Active Directory Federation Service (AD FS)	106 217 251 335 342 349 358 364 381 385 400 401 417 424 435 436
Sysmon	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 255
Microsoft Active Directory Domain Service (AD DS)	1213 1317 1644 2041 2889

Kaspersky Endpoint Security for Linux

В Kaspersky Endpoint Security for Linux, начиная с версии 12.2, есть возможность отправлять события из журналов Linux в коллектор Kaspersky SIEM Cloud. Это позволяет получать в Kaspersky SIEM Cloud события из журналов Linux со всех хостов, на которых установлен Kaspersky Endpoint Security for Linux версии 12.2. Чтобы активировать функциональность, необходимо:

- иметь действующую лицензию Kaspersky SIEM Cloud.
- использовать Kaspersky Security Center 14.2 и выше.
- использовать Kaspersky Endpoint Security for Linux 12.2 или выше.

Настройка получения событий состоит из следующих этапов:

❶ Импорт нормализатора в Kaspersky SIEM Cloud

В Kaspersky SIEM Cloud должно быть настроено получение обновлений через серверы обновлений "Лаборатории Касперского".

В разделе **Ресурсы и сервисы** нажмите **Импорт ресурсов** и выберите **[OOTB] KESL syslog cef** в списке доступных к установке нормализаторов.

❷ Создание коллектора Kaspersky SIEM Cloud для получения событий Linux

При создании коллектора в веб-консоли на шаге **Транспорт** выберите **TCP** или **UDP** и укажите номер порта, который будет прослушивать коллектор. На шаге **Парсинг событий** выберите нормализатор **[OOTB] KESL syslog cef**.

❸ Запрос ключа в Службе технической поддержки

Если в вашей лицензии не было ключа активации функционала отправки журналов Linux в коллектор Kaspersky SIEM Cloud, направьте в Службу технической поддержки письмо следующего содержания: "У нас приобретена лицензия Kaspersky SIEM Cloud и используется Kaspersky Endpoint Security for Linux версии 12.2. Мы планируем активировать функционал отправки журналов Linux в коллектор Kaspersky SIEM Cloud. Просим предоставить файл ключа для активации соответствующего функционала". Новым пользователям Kaspersky SIEM Cloud не требуется писать запрос в Службу технической поддержки, поскольку новым пользователям будет предоставлено двумя ключа с лицензиями для Kaspersky SIEM Cloud и для активации функциональности Kaspersky Endpoint Security for Linux.

В ответ на письмо вам будет предоставлен файл ключа.

❹ Настройка на стороне Kaspersky Security Center и Kaspersky Endpoint Security for Linux

Файл ключа, активирующий функционал отправки событий Linux в коллекторы Kaspersky SIEM Cloud, необходимо импортировать в Kaspersky Security Center и распространить по конечным устройствам Kaspersky Security Center в соответствии с инструкцией. Также необходимо в политике Kaspersky Security Center добавить адреса серверов Kaspersky SIEM Cloud и настроить сетевые параметры подключения.

❺ Проверка поступления событий Linux в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий Linux выполнена правильно, выполнив поиск связанных событий.

Kaspersky Endpoint Security for Linux передает следующие события:

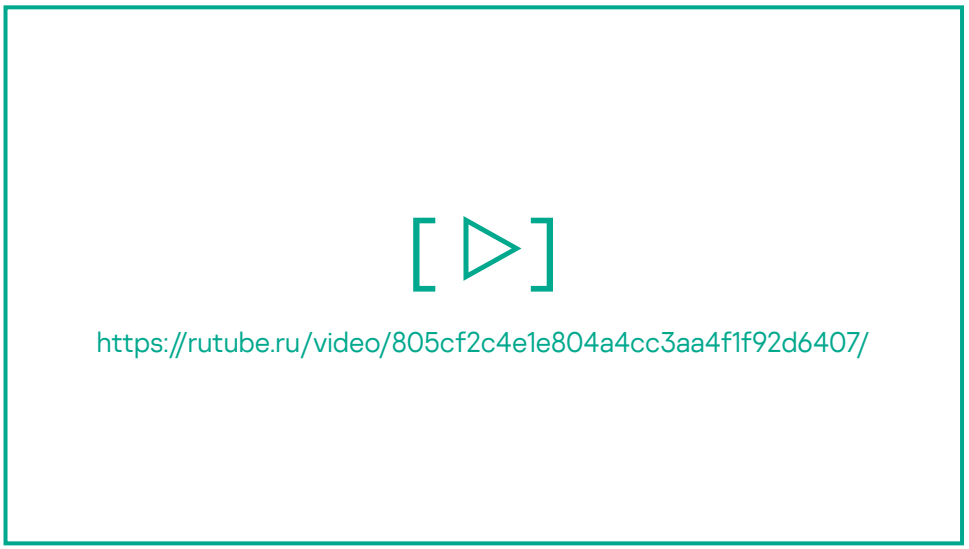
- ProcessCreate
- ProcessTerminate
- FileChange
- New user account created
- User account deleted
- Group created
- Group deleted
- New member added to a group
- Member removed from the group
- User password changed
- Linux authentication performed
- Linux session started
- Linux session finished
- Service started
- Service stopped
- Promiscuous mode modified
- Audit configuration changed
- Account expiration date changed

Microsoft

В этом разделе описана настройка получения событий от продуктов Microsoft, включая Windows и облачные сервисы Microsoft 365.

Агент Kaspersky SIEM Cloud (WEC)

Для наглядного ознакомления с процедурой получения информации о событиях с устройств Windows с помощью агента Kaspersky SIEM Cloud типа WEC вы можете просмотреть видео ниже, а затем воспользоваться пошаговой инструкцией.



https://rutube.ru/video/805cf2c4e1e804a4cc3aa4f1f92d6407/

Настройка получения информации о событиях с устройств Windows с помощью агента Kaspersky SIEM Cloud типа WEC состоит из следующих этапов:

1. Настройка параметров аудита для работы с Kaspersky SIEM Cloud

Вы можете настроить аудит событий на устройствах Windows как на конкретном устройстве, так и на всех устройствах в домене, используя одну из следующих инструкций:

Настройка политики аудита на устройстве Windows

Чтобы настроить политики аудита на устройстве:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.
2. В открывшемся окне введите запрос `secpol.msc` и нажмите **OK**.

   Откроется окно **Локальная политика безопасности**.
3. Перейдите в раздел **Параметры безопасности** → **Локальные политики** → **Политика аудита**.
4. В панели справа двойным щелчком мыши откройте свойства политики, для которой вы хотите включить аудит успешных и неуспешных попыток.
5. В окне **Свойства <Имя политики>** на вкладке **Параметр локальной безопасности** установите флажки **Успех** и **Отказ**, чтобы отслеживать успешные и прерванные попытки.

   Рекомендуется включить аудит успешных и неуспешных попыток для следующих политик:

   - Аудит входа в систему
   - Аудит изменения политики
   - Аудит системных событий

- Аудит событий входа в систему
- Аудит управления учетными записями

Настройка политики аудита на устройстве завершена.

Настройка аудита с помощью групповой политики

Чтобы настроить аудит с помощью групповой политики:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.
2. В открывшемся окне введите запрос `gpedit.msc` и нажмите **OK**.

   Откроется окно **Редактор локальной групповой политики**.
3. Перейдите в раздел **Конфигурация компьютера** → **Конфигурация Windows** → **Параметры безопасности** → **Локальные политики** → **Политика аудита**.
4. В панели справа двойным щелчком мыши откройте свойства политики, для которой вы хотите включить аудит успешных и неуспешных попыток.
5. В окне **Свойства <Имя политики>** на вкладке **Параметр локальной безопасности** установите флажки **Успех** и **Отказ**, чтобы отслеживать успешные и прерванные попытки.

   Рекомендуется включить аудит успешных и неуспешных попыток для следующих политик:

   - Аудит входа в систему
   - Аудит изменения политики
   - Аудит системных событий
   - Аудит событий входа в систему
   - Аудит управления учетными записями

Если вы хотите получать журналы Windows с большого количества серверов или если установка агентов Kaspersky SIEM Cloud на контроллеры домена не допускается, рекомендуется настроить перенаправление журналов Windows на отдельные серверы с настроенной службой Windows Event Collector.

Настройка политики аудита на сервере или рабочей станции завершена.

❷ Настройка централизованного получения событий с помощью службы Windows Event Collector

Служба Windows Event Collector позволяет централизованно получать данные о событиях на серверах и рабочих станциях под управлением ОС Windows. С помощью службы Windows Event Collector вы можете подписаться на события, которые регистрируются на удаленных устройствах.

Вы можете настроить следующие типы подписок на события:

- **Source-initiated subscriptions**. Удаленные устройства отправляют данные о событиях на сервер Windows Event Collector, адрес которого указывается в групповой политике.

  Настройка передачи данных с сервера источника событий

Вы можете получать информацию о событиях на серверах и рабочих станциях, настроив передачу данных с удаленных устройств на сервер Windows Event Collector.

Предварительная подготовка

1. Проверьте, что служба Windows Remote Management настроена на сервере источника событий, выполнив следующую команду в консоли PowerShell:

   ```
   winrm get winrm/config
   ```

   Если служба Windows Remote Management не настроена, инициализируйте ее, выполнив следующую команду:

   ```
   winrm quickconfig
   ```

2. Если сервер источника событий является контроллером домена, откройте доступ по сети к журналам Windows, выполнив следующую команду в консоли PowerShell, запущенной от имени администратора:

   ```
   wevtutil set-log security /ca:'O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;S-1-5-20)'
   ```

   Проверьте наличие доступа, выполнив следующую команду:

   ```
   wevtutil get-log security
   ```

Настройка брандмауэра сервера источника событий

Для того чтобы сервер Windows Event Collector мог получать записи журналов Windows, требуется открыть порты для входящих соединений на сервере источника событий.

Чтобы открыть порты для входящих соединений:

1. На сервере источника событий откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.

2. В открывшемся окне введите запрос `wf.msc` и нажмите **OK**.

   Откроется окно **Монитор брандмауэра Защитника Windows в режиме повышенной безопасности**.

3. Перейдите в раздел **Правила для входящих подключений** и в панели **Действия** нажмите **Создать правило**.

   Откроется **Мастер создания правила для нового входящего пользователя**.

4. На шаге **Тип правила** выберите **Для порта**.

5. На шаге **Протоколы и порты** в качестве протокола выберите **Протокол TCP**. В поле **Определенные локальные порты** укажите номера портов:

   - `5985` (для доступа по HTTP)
   - `5986` (для доступа по HTTPS)

   Вы можете указать один из портов или оба.

6. На шаге **Действие** выберите **Разрешить подключение** (выбрано по умолчанию).

7. На шаге **Профиль** снимите флажки **Частный** и **Публичный**.

8. На шаге **Имя** укажите имя правила для нового входящего подключения и нажмите **Готово**.

Настройка передачи данных с сервера источника событий завершена.

Сервер Windows Event Collector должен обладать правами для чтения журналов Windows на сервере источника событий. Права могут быть предоставлены как учетной записи сервера Windows Event Collector, так и специальной пользовательской учетной записи. Подробнее о предоставлении прав см. в разделе Предоставление прав пользователю для просмотра журнала событий Windows.

- **Collector-initiated subscriptions**. Сервер Windows Event Collector подключается к удаленным устройствам и самостоятельно забирает события из локальных журналов.

  Настройка сервиса получения событий Windows

  Сервер Windows Event Collector может самостоятельно подключаться к устройствам и забирать данные о событиях любого уровня важности.

  Чтобы настроить получение данных о событиях сервером Windows Event Collector:

  1. На сервере-источнике событий откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.
  2. В открывшемся окне введите запрос `services.msc` и нажмите **OK**.

     Откроется окно **Службы**.
  3. В списке служб найдите службу **Сборщик событий Windows** и запустите ее.
  4. Откройте оснастку **Просмотр событий**, выполнив следующие действия:

     a. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.

     b. В открывшемся окне введите запрос `eventvwr` и нажмите **OK**.
  5. Перейдите в раздел **Подписки** и в панели **Действия** нажмите **Создать подписку**.
  6. В открывшемся окне **Свойства подписки** задайте имя и описание подписки, а также следующие параметры:

     a. В поле **Конечный журнал** выберите из списка **Перенаправленные события**.

     b. В разделе **Тип подписки и исходные компьютеры** нажмите на кнопку **Выбрать компьютеры**.

     c. В открывшемся окне **Компьютеры** нажмите на кнопку **Добавить доменный компьютер**.

        Откроется окно **Выбор: "Компьютер"**.

     d. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена устройств, с которых вы хотите получать информацию о событиях. Нажмите **OK**.

     e. В окне **Компьютеры** проверьте список устройств, с которых сервер Windows Event Collector будет забирать данные о событиях и нажмите **OK**.

     f. В окне **Свойства подписки** в поле **Собираемые события** нажмите на кнопку **Выбрать события**.

g. В открывшемся окне **Фильтр запроса** укажите, как часто и какие данные о событиях на устройствах вы хотите получать.

h. При необходимости в поле **<Все коды событий>** перечислите коды событий, информацию о которых вы хотите или не хотите получать. Нажмите **OK**.

7. Если вы хотите использовать специальную учетную запись для просмотра данных о событиях, выполните следующие действия:

a. В окне **Свойства подписки** нажмите на кнопку **Дополнительно**.

b. В открывшемся окне **Дополнительные параметры подписки** в настройках учетной записи пользователя выберите **Определенный пользователь**.

c. Нажмите на кнопку **Пользователь и пароль** и задайте учетные данные выбранного пользователя.

Настройка сервиса получения событий завершена.

Чтобы проверить, что настройка выполнена правильно и данные о событиях поступают на сервер Windows Event Collector,

в оснастке **Просмотр событий** перейдите в раздел **Просмотр событий (Локальный)** → **Журналы Windows** → **Перенаправленные события**.

❸ Предоставление прав для просмотра событий

Вы можете предоставить права для просмотра событий Windows как для конкретного устройства, так и для всех устройств в домене.

Предоставление прав для просмотра событий на конкретном устройстве

Чтобы предоставить права для просмотра событий на конкретном устройстве:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win+R**.
2. В открывшемся окне введите запрос `compmgmt.msc` и нажмите **OK**.

   Откроется окно **Управление компьютером**.
3. Перейдите в раздел **Управление компьютером (локальным)** → **Локальные пользователи и группы** → **Группы**.
4. В панели справа выберите группу **Читатели журнала событий** и двойным щелчком мыши откройте свойства политики.
5. Внизу окна **Свойства: Читатели журнала событий** нажмите на кнопку **Добавить**.

   Откроется окно **Выбор пользователя, компьютера или группы**.
6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить права для просмотра данных о событиях.
7. Нажмите **OK**.

Предоставление прав для просмотра событий всех устройств в домене

Чтобы предоставить права для просмотра событий всех устройств в домене:

1. Зайдите в контроллер домена с правами администратора.
2. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.
3. В открывшемся окне введите запрос `dsa.msc` и нажмите **OK**.

   Откроется окно **Active Directory Пользователи и Компьютеры**.
4. Перейдите в раздел **Active Directory Пользователи и Компьютеры** → **<Имя домена>** → **Builtin**.
5. В панели справа выберите группу **Читатели журнала событий** и двойным щелчком мыши откройте свойства политики.

   В окне **Свойства: Читатели журнала событий** откройте вкладку **Члены** и нажмите на кнопку **Добавить**.

   Откроется окно **Выбор пользователя, компьютера или группы**.
6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить права для просмотра данных о событиях.
7. Нажмите **OK**.

4 Предоставление прав входа в качестве службы

Вы можете предоставить право на вход в систему в качестве службы как конкретному устройству, так и всем устройствам в домене. Право входа в систему в качестве службы позволяет запустить процесс от имени учетной записи, которой это право предоставлено.

Предоставление прав на вход в качестве службы конкретному устройству

> Перед предоставлением права убедитесь, что учетные записи или устройства, которым вы собираетесь предоставить право **Вход в качестве службы**, отсутствуют в свойствах политики **Отказ во входе в качестве службы**.

Чтобы предоставить право на вход в качестве службы устройству:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.
2. В открывшемся окне введите запрос `secpol.msc` и нажмите **OK**.

   Откроется окно **Локальная политика безопасности**.
3. Перейдите в раздел **Параметры безопасности** → **Локальные политики** → **Назначение прав пользователя**.
4. В панели справа двойным щелчком мыши откройте свойства политики **Вход в качестве службы**.
5. В открывшемся окне **Свойства: Вход в качестве службы** нажмите на кнопку **Добавить Пользователя или Группу**.

   Откроется окно **Выбор пользователей или групп**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена учетных записей или устройств, которым вы хотите предоставить право входа в систему в качестве службы.

7. Нажмите **OK**.

Предоставление прав на вход в качестве службы всем устройствам в домене

> Перед предоставлением права убедитесь, что учетные записи или устройства, которым вы собираетесь предоставить право **Вход в качестве службы**, отсутствуют в свойствах политики **Отказ во входе в качестве службы**.

Чтобы предоставить право на вход в качестве службы устройствам в домене:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.

2. В открывшемся окне введите запрос `gpedit.msc` и нажмите **OK**.

   Откроется окно **Редактор локальной групповой политики**.

3. Перейдите в раздел **Конфигурация компьютера** → **Конфигурация Windows** → **Параметры безопасности** → **Локальные политики** → **Назначение прав пользователя**.

4. В панели справа двойным щелчком мыши откройте свойства политики **Вход в качестве службы**.

5. В открывшемся окне **Свойства: Вход в качестве службы** нажмите на кнопку **Добавить Пользователя или Группу**.

   Откроется окно **Выбор пользователей или групп**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить право входа в систему в качестве службы.

7. Нажмите **OK**.

❺ Создание коллектора Kaspersky SIEM Cloud для получения событий с устройств Windows

Создайте коллектор в веб-интерфейсе Kaspersky SIEM Cloud для событий с устройств Windows, указав следующие параметры коллектора:

1. На шаге **Транспорт** укажите следующие параметры:

   a. В поле **Коннектор** выберите **Создать**.

   b. В поле **Тип** выберите **http**.

   c. В поле **Разделитель** выберите **\0**.

2. На вкладке **Дополнительные параметры** в поле **Режим TLS** выберите **Включено**.

3. На шаге **Парсинг событий** нажмите на кнопку **Добавить парсинг событий**.

4. В открывшемся окне **Основной парсинг событий** в поле **Нормализатор** выберите **[OOTB] Microsoft Products** и нажмите **OK**.

5. На шаге **Маршрутизация** добавьте следующие точки назначения:

   - **Хранилище**. Для отправки обработанных событий в хранилище.
   - **Коррелятор**. Для отправки обработанных событий в коррелятор.

   Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

6. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

7. Скопируйте появившуюся команду для установки коллектора Kaspersky SIEM Cloud.

❻ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для получения событий с устройств Windows требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

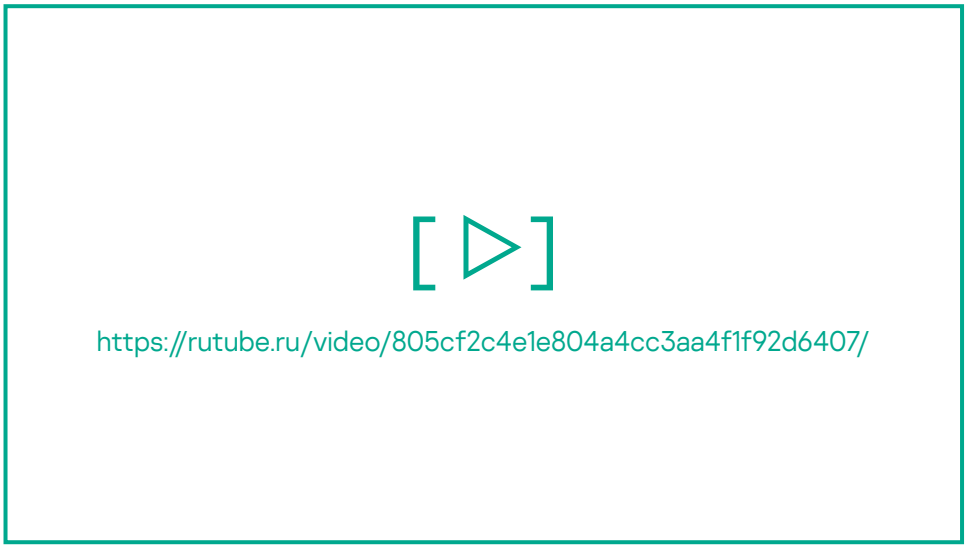
❼ Передача событий с устройств Windows в Kaspersky SIEM Cloud

Чтобы завершить настройку передачи данных, требуется создать агент Kaspersky SIEM Cloud типа WEC, а затем установить его на устройстве, с которого вы хотите получать информацию о событиях.

Подробнее о создании и установке агента Kaspersky SIEM Cloud типа WEC на устройства Windows см. в разделе Передача в Kaspersky SIEM Cloud событий с устройств Windows.

Агент Kaspersky SIEM Cloud (WMI)

Для наглядного ознакомления с процедурой получения информации о событиях с устройств Windows с помощью агента Kaspersky SIEM Cloud типа WMI вы можете просмотреть видео ниже, а затем воспользоваться пошаговой инструкцией.



https://rutube.ru/video/805cf2c4e1e804a4cc3aa4f1f92d6407/

Настройка получения информации о событиях с устройств Windows с помощью агента Kaspersky SIEM Cloud типа WMI состоит из следующих этапов:

1 Настройка параметров аудита для работы с Kaspersky SIEM Cloud

Вы можете настроить аудит событий на устройствах Windows как на конкретном устройстве, так и на всех устройствах в домене, используя одну из следующих инструкций:

Настройка политики аудита на конкретном устройстве Windows

Чтобы настроить политики аудита на устройстве:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.
2. В открывшемся окне введите запрос `secpol.msc` и нажмите **OK**.

   Откроется окно **Локальная политика безопасности**.
3. Перейдите в раздел **Параметры безопасности** → **Локальные политики** → **Политика аудита**.
4. В панели справа двойным щелчком мыши откройте свойства политики, для которой вы хотите включить аудит успешных и неуспешных попыток.
5. В окне **Свойства <Имя политики>** на вкладке **Параметр локальной безопасности** установите флажки **Успех** и **Отказ**, чтобы отслеживать успешные и прерванные попытки.

   Рекомендуется включить аудит успешных и неуспешных попыток для следующих политик:

   - Аудит входа в систему
   - Аудит изменения политики
   - Аудит системных событий
   - Аудит событий входа в систему
   - Аудит управления учетными записями

Настройка политики аудита на устройстве завершена.

Настройка аудита с помощью групповой политики

Чтобы настроить аудит с помощью групповой политики:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.
2. В открывшемся окне введите запрос `gpedit.msc` и нажмите **OK**.

   Откроется окно **Редактор локальной групповой политики**.
3. Перейдите в раздел **Конфигурация компьютера** → **Конфигурация Windows** → **Параметры безопасности** → **Локальные политики** → **Политика аудита**.
4. В панели справа двойным щелчком мыши откройте свойства политики, для которой вы хотите включить аудит успешных и неуспешных попыток.
5. В окне **Свойства <Имя политики>** на вкладке **Параметр локальной безопасности** установите флажки **Успех** и **Отказ**, чтобы отслеживать успешные и прерванные попытки.

Рекомендуется включить аудит успешных и неуспешных попыток для следующих политик:

- Аудит входа в систему
- Аудит изменения политики
- Аудит системных событий
- Аудит событий входа в систему
- Аудит управления учетными записями

Если вы хотите получать журналы Windows с большого количества серверов или если установка агентов Kaspersky SIEM Cloud на контроллеры домена не допускается, рекомендуется настроить перенаправление журналов Windows на отдельные серверы с настроенной службой Windows Event Collector.

Настройка политики аудита на сервере или рабочей станции завершена.

❷ Предварительная подготовка перед настройкой передачи данных с сервера источника событий

1. На сервере источника событий откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.
2. В открывшемся окне введите запрос:

   ```
   services.msc
   ```

3. Нажмите **OK**.

   Откроется окно **Службы**.
4. В списке служб найдите следующие службы:
   - **Удаленный вызов процедур**.
   - **Сопоставитель конечных точек RPC**.
5. Убедитесь, что в графе **Состояние** у этих служб отображается статус **Выполняется**.

❸ Настройка брандмауэра сервера источника событий

Сервер Windows Management Instrumentation может получать записи журналов Windows, если открыты порты для входящих соединений на сервере источника событий.

Чтобы открыть порты для входящих соединений:

1. На сервере источника событий откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.
2. В открывшемся окне введите запрос:

   ```
   wf.msc
   ```

3. Нажмите **OK**.

4. В открывшемся окне **Монитор брандмауэра Защитника Windows в режиме повышенной безопасности** перейдите в раздел **Правила для входящих подключений** и в панели **Действия** нажмите **Создать правило**.

   Откроется **Мастер создания правила для нового входящего подключения**.

5. На шаге **Тип правила** выберите **Для порта**.

6. На шаге **Протоколы и порты** в качестве протокола выберите **Протокол TCP** и в поле **Определенные локальные порты** укажите номера портов:

   - 135
   - 445
   - 49152–65535

7. На шаге **Действие** выберите **Разрешить подключение** (выбрано по умолчанию).

8. На шаге **Профиль** снимите флажки **Частный** и **Публичный**.

9. На шаге **Имя** укажите имя правила для нового входящего подключения.

10. Нажмите **Готово**.

    Настройка передачи данных с сервера источника событий завершена.

Если порты закрыты, возвращается ошибка The RPC server is unavailable.

4 Предоставление прав для просмотра событий

Вы можете предоставить права для просмотра событий Windows как для конкретного устройства, так и для всех устройств в домене.

Предоставление прав для просмотра событий на конкретном устройстве

Чтобы предоставить права для просмотра событий на конкретном устройстве:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win+R**.

2. В открывшемся окне введите запрос `compmgmt.msc` и нажмите **OK**.

   Откроется окно **Управление компьютером**.

3. Перейдите в раздел **Управление компьютером (локальным)** → **Локальные пользователи и группы** → **Группы**.

4. В панели справа выберите группу **Читатели журнала событий** и двойным щелчком мыши откройте свойства политики.

5. Внизу окна **Свойства: Читатели журнала событий** нажмите на кнопку **Добавить**.

   Откроется окно **Выбор пользователя, компьютера или группы**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить права для просмотра данных о событиях.

7. Нажмите **OK**.

Предоставление прав для просмотра событий всех устройств в домене

Чтобы предоставить права для просмотра событий всех устройств в домене:

1. Зайдите в контроллер домена с правами администратора.

2. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.

3. В открывшемся окне введите запрос `dsa.msc` и нажмите **OK**.

   Откроется окно **Active Directory Пользователи и Компьютеры**.

4. Перейдите в раздел **Active Directory Пользователи и Компьютеры** → **<Имя домена>** → **Builtin**.

5. В панели справа выберите группу **Читатели журнала событий** и двойным щелчком мыши откройте свойства политики.

   В окне **Свойства: Читатели журнала событий** откройте вкладку **Члены** и нажмите на кнопку **Добавить**.

   Откроется окно **Выбор пользователя, компьютера или группы**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить права для просмотра данных о событиях.

7. Нажмите **OK**.

❺ Предоставление прав входа в качестве службы

Вы можете предоставить право на вход в систему в качестве службы как конкретному устройству, так и всем устройствам в домене. Право входа в систему в качестве службы позволяет запустить процесс от имени учетной записи, которой это право предоставлено.

Предоставление прав на вход в качестве службы конкретному устройству

> Перед предоставлением права убедитесь, что учетные записи или устройства, которым вы собираетесь предоставить право **Вход в качестве службы**, отсутствуют в свойствах политики **Отказ во входе в качестве службы**.

Чтобы предоставить право на вход в качестве службы устройству:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win**+**R**.

2. В открывшемся окне введите запрос `secpol.msc` и нажмите **OK**.

   Откроется окно **Локальная политика безопасности**.

3. Перейдите в раздел **Параметры безопасности** → **Локальные политики** → **Назначение прав пользователя**.

4. В панели справа двойным щелчком мыши откройте свойства политики **Вход в качестве службы**.

5. В открывшемся окне **Свойства: Вход в качестве службы** нажмите на кнопку **Добавить Пользователя или Группу**.

   Откроется окно **Выбор пользователей или групп**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена учетных записей или устройств, которым вы хотите предоставить право входа в систему в качестве службы.

7. Нажмите **OK**.

Предоставление прав на вход в качестве службы всем устройствам в домене

Перед предоставлением права убедитесь, что учетные записи или устройства, которым вы собираетесь предоставить право **Вход в качестве службы**, отсутствуют в свойствах политики **Отказ во входе в качестве службы**.

Чтобы предоставить право на вход в качестве службы устройствам в домене:

1. Откройте окно **Выполнить**, нажав комбинацию клавиш **Win+R**.

2. В открывшемся окне введите запрос `gpedit.msc` и нажмите **OK**.

   Откроется окно **Редактор локальной групповой политики**.

3. Перейдите в раздел **Конфигурация компьютера → Конфигурация Windows → Параметры безопасности → Локальные политики → Назначение прав пользователя**.

4. В панели справа двойным щелчком мыши откройте свойства политики **Вход в качестве службы**.

5. В открывшемся окне **Свойства: Вход в качестве службы** нажмите на кнопку **Добавить Пользователя или Группу**.

   Откроется окно **Выбор пользователей или групп**.

6. В поле **Введите имена выбираемых объектов (примеры)** перечислите имена пользователей или устройств, которым вы хотите предоставить право входа в систему в качестве службы.

7. Нажмите **OK**.

6 Создание коллектора Kaspersky SIEM Cloud для получения событий с устройств Windows

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] Microsoft Products**.

7 Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для получения событий с устройств Windows требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

8 Передача событий с устройств Windows в Kaspersky SIEM Cloud

Чтобы завершить настройку передачи данных, требуется создать агент Kaspersky SIEM Cloud типа WMI, а затем установить его на устройстве, с которого вы хотите получать информацию о событиях.

Подробнее о создании и установке агента Kaspersky SIEM Cloud типа WMI на устройства Windows см. в разделе Передача в Kaspersky SIEM Cloud событий с устройств Windows.

Коннектор Event Tracing for Windows

Коннектор Event Tracing for Windows (далее также коннектор ETW) – это механизм ведения журнала событий, создаваемых приложениями и драйверами на DNS-сервере. Вы можете использовать коннектор ETW для устранения ошибок при разработке, а также для поиска вредоносной активности.

Использование коннектора ETW оказывает незначительное влияние на производительность DNS-сервера. Например, DNS-сервер, который работает на современном оборудовании и получает до 100 000 запросов в секунду (англ. queries per second, QPS), может испытывать снижение производительности на 5% при использовании коннектора ETW. Если DNS-сервер получает до 50 000 запросов в секунду, снижение производительности не наблюдается. Мы рекомендуем следить за производительностью DNS-сервера при использовании коннектора ETW вне зависимости от количества запросов в секунду.

По умолчанию вы можете использовать коннектор ETW на операционной системе Windows Server, начиная с версии Windows Server 2016. Коннектор ETW также поддерживается версией Windows Server 2012 R2, если установлено исправление для ведения журнала событий и аудита изменений. Исправление доступно на сайте службы технической поддержки Microsoft.

Коннектор ETW состоит из следующих компонентов:

- *Поставщики* или *провайдеры* (англ. providers) – элементы системы, которые генерируют события и отправляют их коннектору ETW. Например, поставщиками могут быть ядра Windows или драйвера устройств. При работе с кодом разработчикам нужно указать, какие события поставщики отправляют коннектору ETW. Событием может быть выполнение важной с точки зрения разработчика функции, например функции, которая открывает доступ к Security Account Manager (SAM).

- *Потребители* (англ. consumers) – программные системы, получают от коннектора ETW события, сгенерированные поставщиками, после чего используют эти события. Например, потребителем может быть Kaspersky SIEM Cloud.

- *Контроллеры* (англ. controllers) – программы, которые управляют взаимодействием между поставщиками и потребителями. Например, контроллерами могут быть утилиты Logman или Wevtutil. Поставщики регистрируются в контроллере для отправки событий потребителям. Контроллер может включить или выключить поставщика. Если поставщик выключен, он не генерирует события.

Для установки связи между поставщиками и потребителями контроллеры используют сессии трассировки. Сессии трассировки также используются для фильтрации данных по указанным параметрам, так как потребителям могут требоваться разные события.

Настройка получения событий DNS-сервера с помощью коннектора ETW состоит из следующих этапов:

1 Настройка на стороне Windows

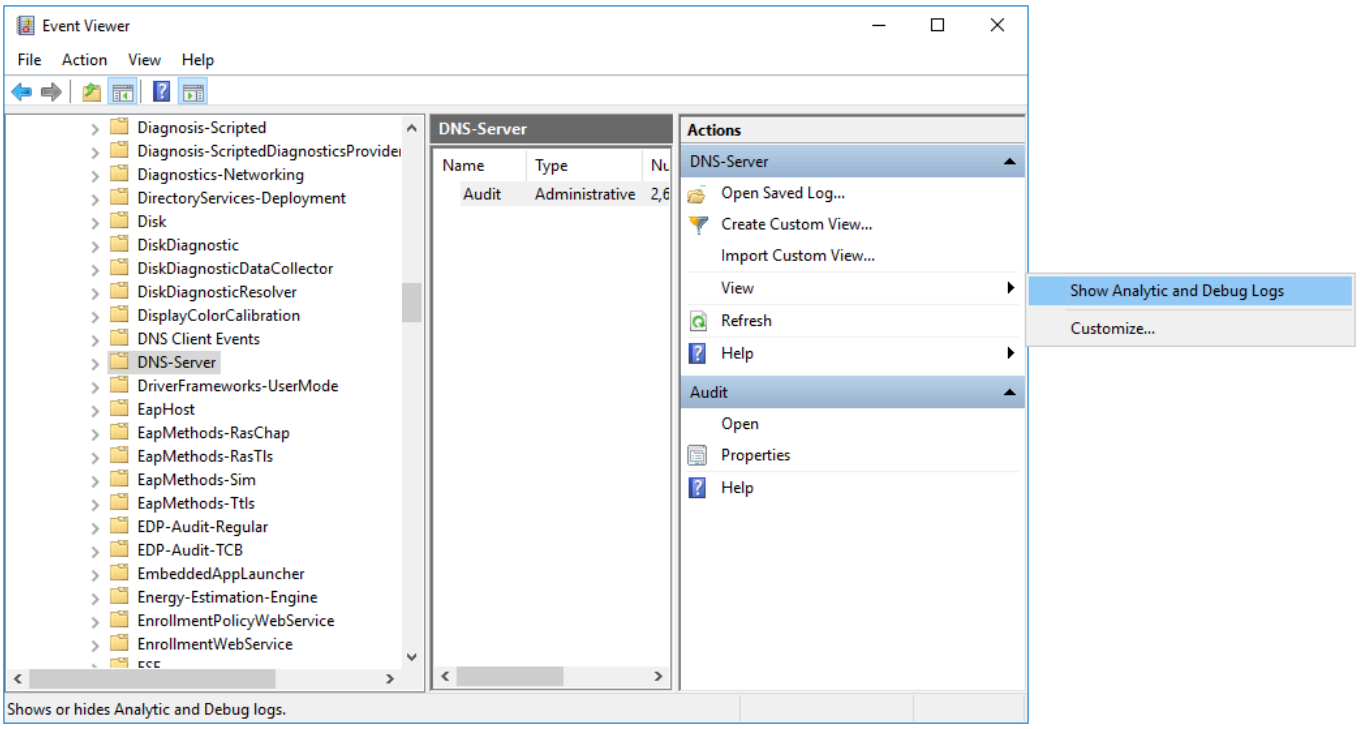
Чтобы настроить получение событий DNS-сервера с помощью коннектора ETW на стороне Windows:

1. Запустите Просмотр событий (англ. Event viewer), выполнив команду:

```
eventvwr.msc
```

2. В открывшемся окне перейдите в директорию **Журналы приложений и служб** → **Microsoft** → **Windows** → **DNS-Server**.

3. Откройте контекстное меню директории **DNS-Server** и выберите пункт **Вид** → **Отобразить аналитический и отладочный журналы**.

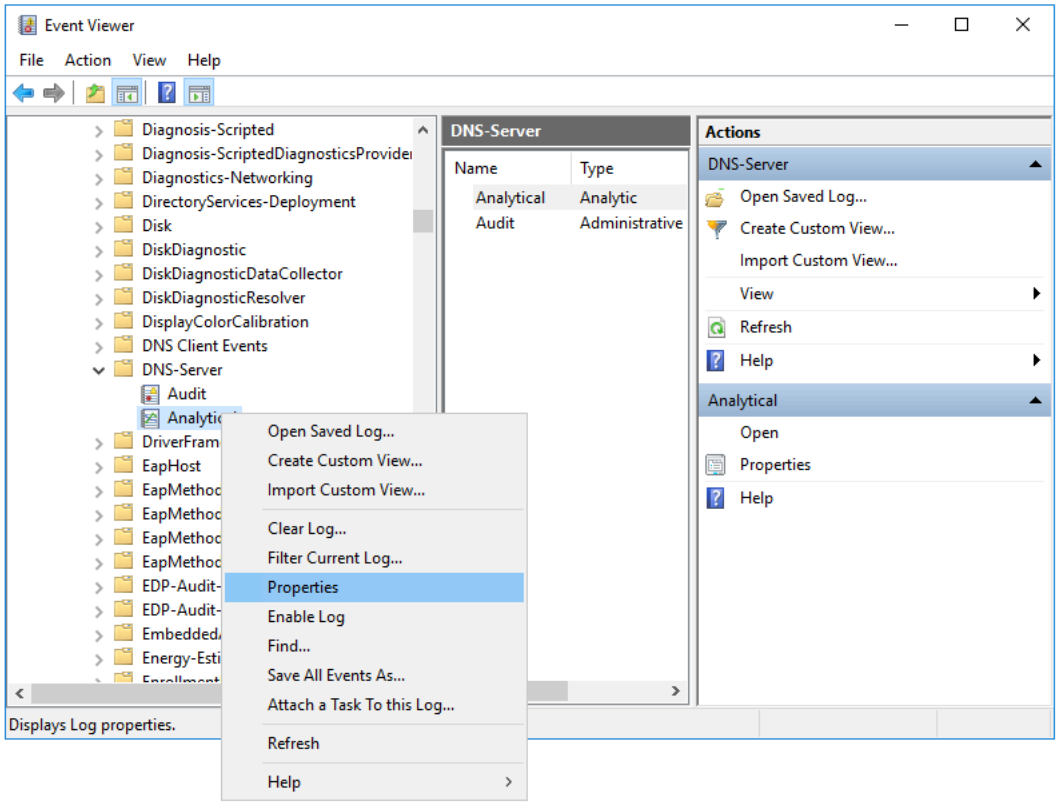


Отображение аналитического и отладочного журнала

Отобразится отладочный журнал **Audit** и аналитический журнал **Analytical**.

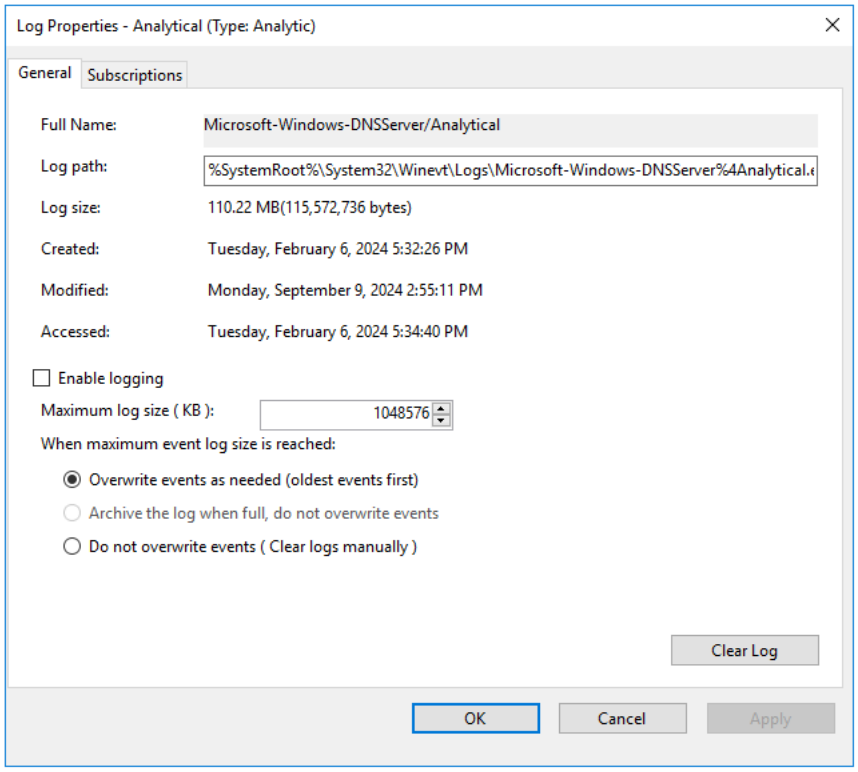
4. Настройте аналитический журнал:

a. Откройте контекстное меню аналитического журнала **Analytical** и выберите пункт **Свойства**.



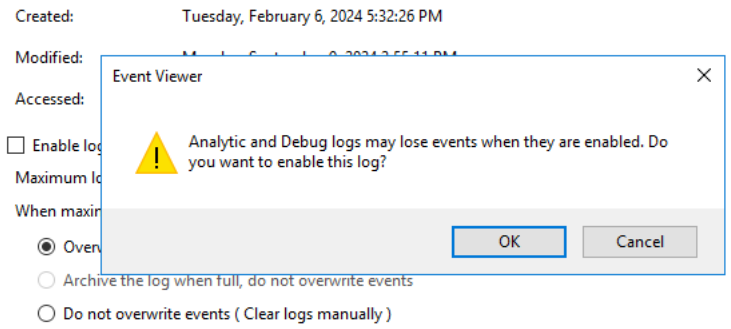
Переход в свойства аналитического журнала Analytical

a. В открывшемся окне убедитесь, что в поле **Макс. размер журнала (КБ)** указано значение `1048576`.



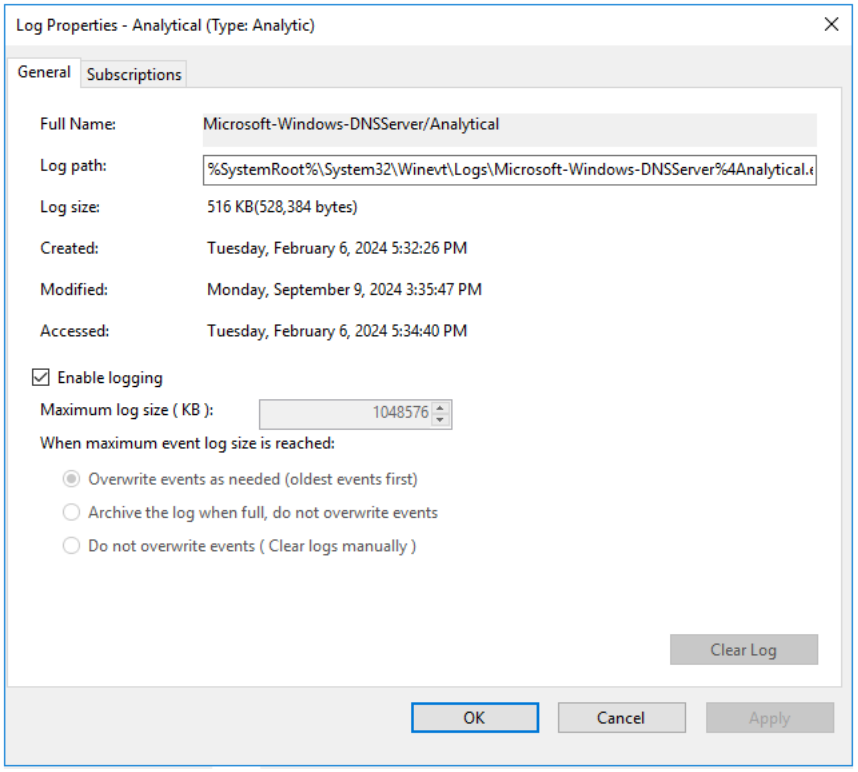
Свойства аналитического журнала Analytical

a. Установите флажок **Включить ведение журнала** и в открывшемся окне подтверждения нажмите на кнопку **OK**.



Окно подтверждения

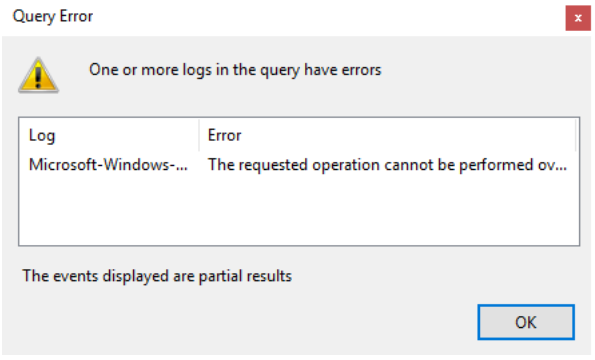
Параметры аналитического журнала должны быть настроены следующим образом:



Проверка корректности параметров аналитического журнала Analytical

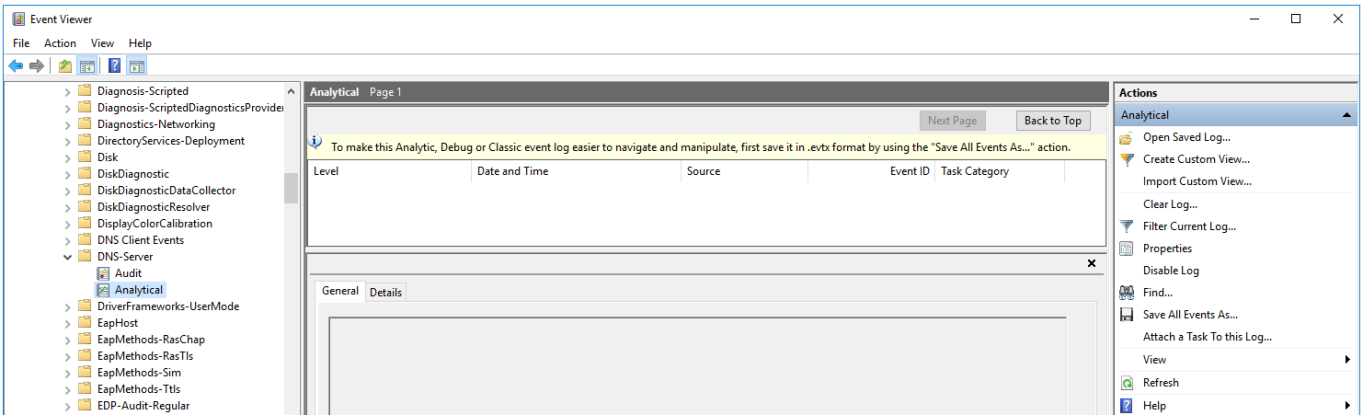
a. Нажмите на кнопку **Применить**, после чего нажмите на кнопку **OK**.

   Отобразится уведомление об ошибке.



Окно ошибки

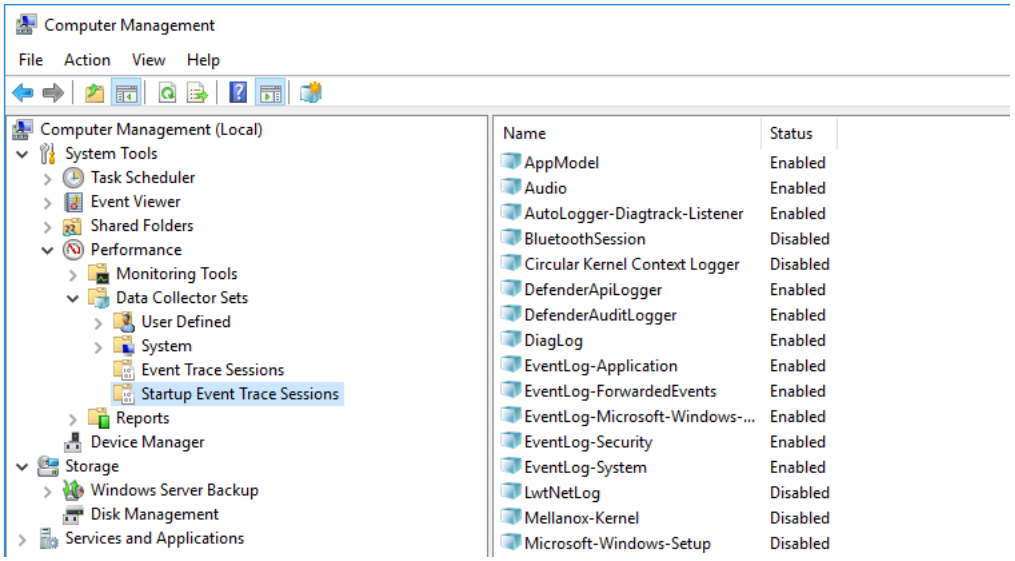
При включенной ротации аналитического журнала события не отображаются. Для просмотра событий в панели **Действия** нажмите на кнопку **Остановить журнал**.



Остановка журнала

5. Запустите Управление компьютером (англ. Computer management) от имени администратора.

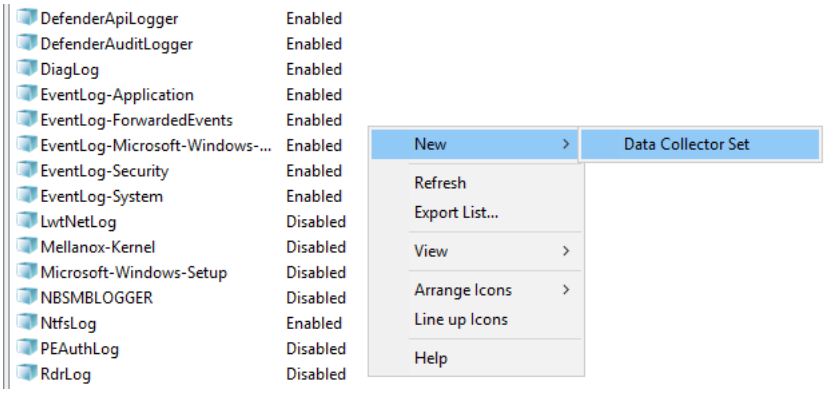
6. В открывшемся окне перейдите в директорию **Служебные программы** → **Производительность** → **Сеансы отслеживания событий запуска**.



Управление компьютером

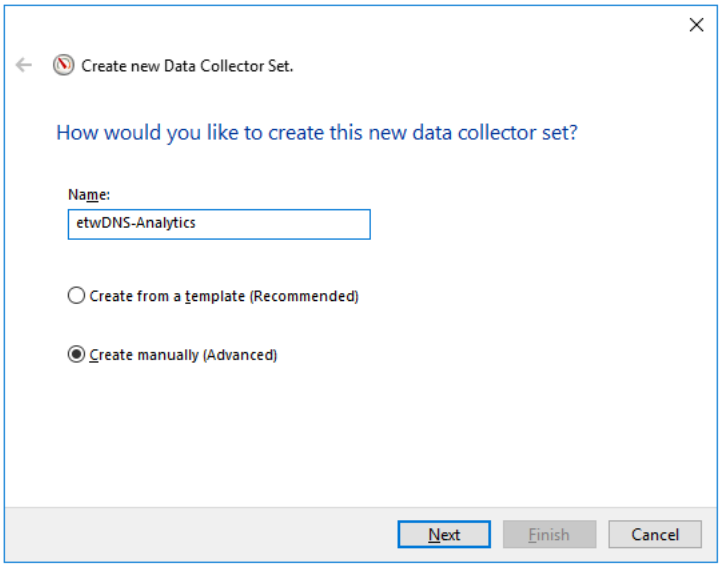
7. Создайте поставщика:

a. Откройте контекстное меню директории **Сеансы отслеживания событий запуска** и выберите пункт **Создать → Группа сборщиков данных**.



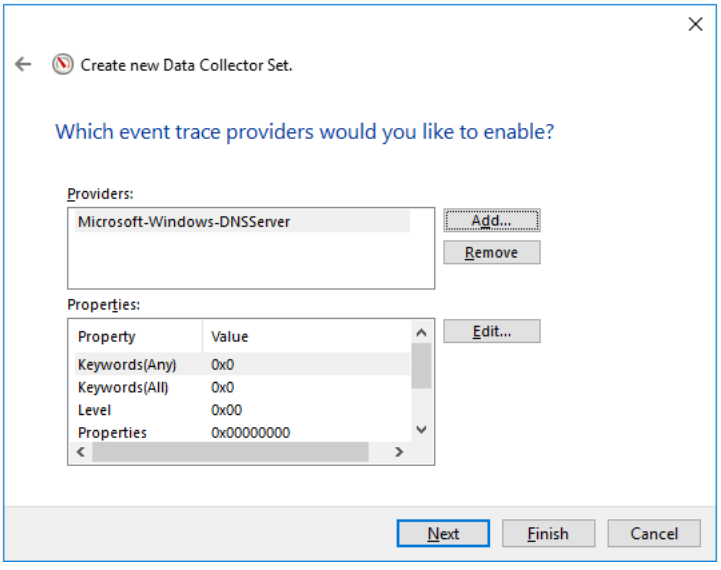
Создание группы сборщиков данных

a. В открывшемся окне введите имя поставщика и нажмите на кнопку **Далее**.



Ввод имени поставщика

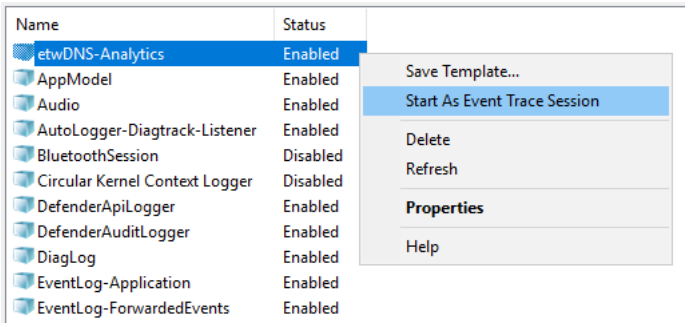
a. Нажмите на кнопку **Добавить...** и в открывшемся окне выберите поставщика **Microsoft-Windows-DNSServer**.



Агент Kaspersky SIEM Cloud с коннектором ETW работает только с System.Provider.Guid: {EB79061A-A566-4698-9119-3ED2807060E7} - Microsoft-Windows-DNSServer.

a. Дважды нажмите на кнопку **Далее**, после чего нажмите на кнопку **Готово**.

8. Откройте контекстное меню созданного поставщика и выберите пункт **Запустить как сеанс отслеживания событий**.



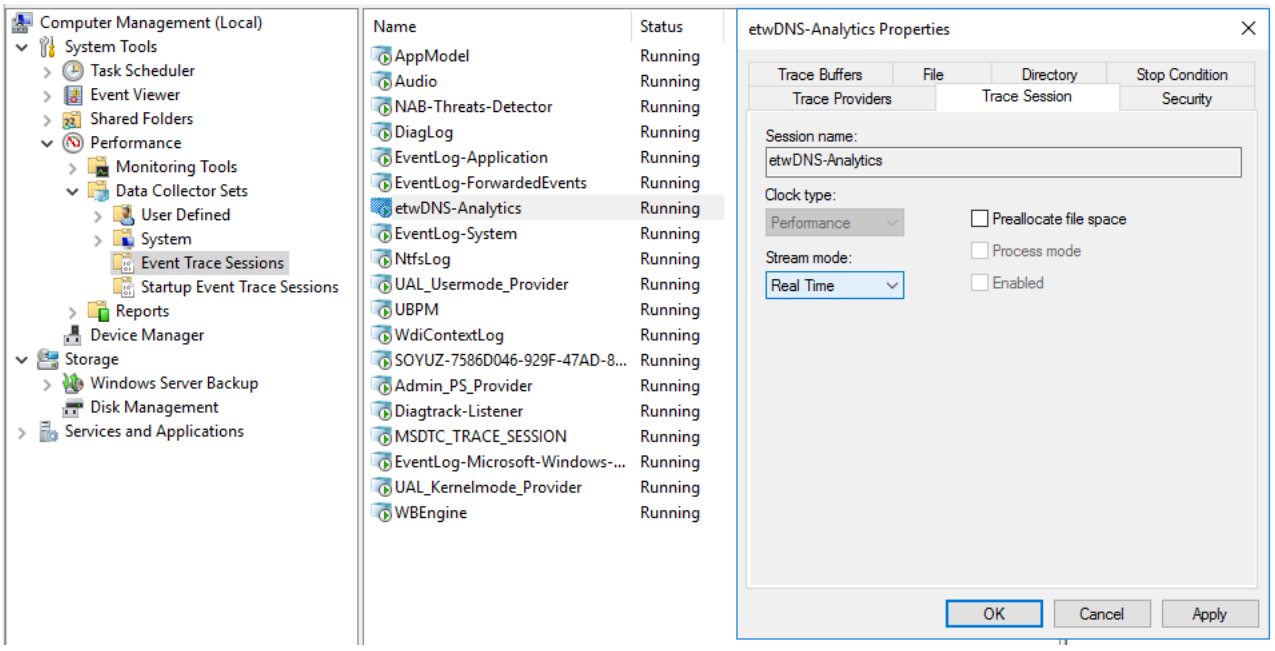
Запуск поставщика

9. Перейдите в директорию **Сеансы отслеживания событий**.

   Отобразятся сеансы отслеживания событий.

10. Откройте контекстное меню созданного сеанса отслеживания событий и выберите пункт **Свойства**.

11. В открывшемся окне выберите вкладку **Сеансы отслеживания** и в раскрывающемся списке **Режим потока** выберите **Режим реального времени**.



Настройка режима потока

12. Нажмите на кнопку **Применить**, после чего нажмите на кнопку **OK**.

Настройка получения событий DNS-сервера с помощью коннектора ETW будет завершена.

❷ Создание коллектора Kaspersky SIEM Cloud для получения событий DNS-сервера с помощью коннектора ETW

При создании коллектора Kaspersky SIEM Cloud выполните следующие действия:

1. На шаге 2 мастера установки коллектора выполните следующие действия:

   a. В раскрывающемся списке **Тип** выберите тип коннектора **tcp** или **http**.

   b. В поле **URL** введите FQDN и номер порта, на котором коллектор Kaspersky SIEM Cloud будет ожидать соединения от агента Kaspersky SIEM Cloud. Вы можете указать номер любого из незанятых портов.

   c. В поле **Разделитель** введите `\n`.

2. На шаге 3 мастера установки коллектора в раскрывающемся списке **Нормализатор** выберите нормализатор. Мы рекомендуем выбрать предустановленный расширенный нормализатор для событий Windows **[OOTB] Microsoft DNS ETW logs json**.

3. На шаге 7 мастера установки коллектора добавьте точку назначения с типом **Хранилище** для хранения событий. Если вы планируете использовать корреляцию по событиям, вам также нужно добавить точку назначения с типом **Коррелятор**.

4. На шаге 8 мастера установки коллектора нажмите на кнопку **Сохранить и создать сервис**, после чего в нижней части окна скопируйте команду для установки коллектора Kaspersky SIEM Cloud на сервере.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

1. Подключитесь к интерфейсу командной строки Kaspersky SIEM Cloud, используя учетную запись пользователя с правами root.

2. Установите коллектор Kaspersky SIEM Cloud, выполнив команду, которую вы скопировали на 8-м шаге мастера установки коллектора.

3. Если вы хотите добавить порт коллектора Kaspersky SIEM Cloud в исключения межсетевого экрана и обновить параметры межсетевого экрана, выполните команды:

```
firewall-cmd --add-port=<collector port number>/tcp –permanent
firewall-cmd --reload
```

Коллектор Kaspersky SIEM Cloud будет установлен, и статус сервиса коллектора Kaspersky SIEM Cloud изменится на зеленый в веб-интерфейсе Kaspersky SIEM Cloud.

❹ Создание агента Kaspersky SIEM Cloud

При создании агента Kaspersky SIEM Cloud выполните следующие действия:

1. Выберите вкладку **Подключение 1**.
2. В блоке параметров **Коннектор** раскрывающемся списке **Коннектор** выберите **Создать** и укажите следующие параметры:
   a. В раскрывающемся списке **Тип** выберите тип коннектора **etw**.
   b. В поле **Имя сессии** введите имя поставщика, которое вы указали при настройке получения событий DNS-сервера с помощью коннектора ETW на стороне Windows.
3. В блоке параметров **Точки назначения** в раскрывающемся списке **Точка назначения** выберите **Создать** и укажите следующие параметры:
   a. В раскрывающемся списке **Тип** выберите тип точки назначения **tcp**.
   b. В поле **URL** введите FQDN и номер порта, на котором коллектор Kaspersky SIEM Cloud будет ожидать соединения от агента Kaspersky SIEM Cloud. Введенное значение должно совпадать со значением, которое вы указали на шаге 2 мастера установки коллектора.
4. Выберите вкладку **Дополнительные параметры** и в поле **Размер дискового буфера** введите:

```
1073741824
```

❺ Создание сервиса агента Kaspersky SIEM Cloud

Вам нужно скопировать идентификатор созданного сервиса агента Kaspersky SIEM Cloud в разделе **Ресурсы → Активные сервисы**. Для этого нажмите на правую кнопку мыши рядом с сервисом агента Kaspersky SIEM Cloud и в контекстном меню выберите пункт **Копировать идентификатор**.

❻ Создание учетной записи для агента Kaspersky SIEM Cloud

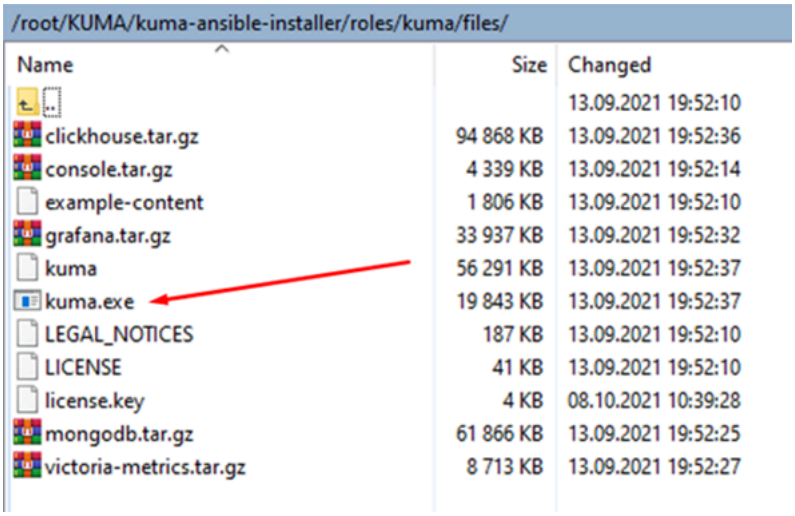
Создайте доменную или локальную учетную запись Windows для запуска агента Kaspersky SIEM Cloud и обеспечения доступа к чтению аналитического журнала. Вам нужно добавить созданную учетную запись в группу пользователей **Пользователи журналов производительности** (англ. **Performance Log Users group**), а также назначить этой учетной записи право **Вход в качестве службы** (англ. **Log on as a service**).

❼ Установка агента Kaspersky SIEM Cloud на Windows-сервере

Вам нужно установить агент Kaspersky SIEM Cloud на Windows-сервере, который будет обеспечивать прием событий от поставщика. Для этого выполните следующие действия:

1. Добавьте FQDN сервера Ядра Kaspersky SIEM Cloud в файл `hosts` на Windows-сервере либо на DNS-сервер.
2. Создайте папку `C:\Users\<имя пользователя>\Desktop\KUMA` на Windows-сервере.

3. Скопируйте файл `kuma.exe` из архива пакетов установки Kaspersky SIEM Cloud в папку `C:\Users\<имя пользователя>\Desktop\KUMA`.



4. Запустите командную строку от имени администратора.

5. Перейдите в папку `C:\Users\<имя пользователя>\Desktop\KUMA` и выполните команду:

```
C:\Users\<user name>\Desktop\KUMA>kuma.exe agent --core https://<DOMAIN-NAME-KUMA-CORE-Server>:7210 --id
<Kaspersky SIEM Cloud agent service ID>
```

В веб-интерфейсе Kaspersky SIEM Cloud в разделе **Ресурсы** → **Активные сервисы** убедитесь, что сервис агента Kaspersky SIEM Cloud был запущен и его статус изменился на зеленый, после чего прервите выполнение команды.

6. Запустите установку агента Kaspersky SIEM Cloud одним из следующих способов:

- Если вы хотите запустить установку агента Kaspersky SIEM Cloud с использованием доменной учетной записи, выполните команду:

```
C:\Users\<user name>\Desktop\KUMA>kuma.exe agent --core https://<DOMAIN-NAME-KUMA-CORE-Server>:7210 --
pair.fingerprint <идентификатор отпечатка CA-сертификата Ядра Kaspersky SIEM Cloud> --id <Kaspersky SIEM
Cloud agent service ID> --user <domain>\<account name for the Kaspersky SIEM Cloud agent> --install
```

- Если вы хотите запустить установку агента с использованием локальной учетной записи, выполните команду:

```
C:\Users\<user name>\Desktop\KUMA>kuma.exe agent --core https://<DOMAIN-NAME-KUMA-CORE-Server>:7210 --
pair.fingerprint <идентификатор отпечатка CA-сертификата Ядра Kaspersky SIEM Cloud> --id <Kaspersky SIEM
Cloud agent service ID> --user <account name for the Kaspersky SIEM Cloud agent> --install
```

где:

`<Kaspersky SIEM Cloud Core CA certificate thumbprint ID>` - идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса.

Параметр `--pair.fingerprint` является необязательным. При создании сервиса Kaspersky SIEM Cloud автоматически добавляет этот параметр в команду установки и указывает идентификатор отпечатка.
Вы можете выполнить установку сервиса без указания параметра `--pair.fingerprint`. В этом случае Kaspersky SIEM Cloud использует значение `insecure` по умолчанию, что не обеспечивает проверку подлинности CA-сертификата Ядра Kaspersky SIEM Cloud при установлении соединения. Если используется значение `insecure`, обновление отпечатка после перевыпуска CA-сертификата не требуется.

Для обеспечения проверки подлинности CA-сертификата Ядра Kaspersky SIEM Cloud рекомендуется не удалять параметр `--pair.fingerprint` с идентификатором отпечатка при установке сервиса. При перевыпуске CA-сертификата необходимо скопировать новый отпечаток сертификата в веб-интерфейсе и перезапустить сервис с обновленным значением параметра.

Вам потребуется ввести пароль учетной записи для агента Kaspersky SIEM Cloud.

На Windows-сервере будет установлен сервис KUMA Windows Agent <идентификатор сервиса агента Kaspersky SIEM Cloud>. Если в веб-интерфейсе Kaspersky SIEM Cloud в разделе **Ресурсы → Активные сервисы** сервис агента Kaspersky SIEM Cloud не запущен и имеет красный статус, вам нужно убедиться в доступности портов 7210, а также порта коллектора Windows по направлению от агента Kaspersky SIEM Cloud к коллектору Kaspersky SIEM Cloud.

Для удаления сервиса агента Kaspersky SIEM Cloud на Windows-сервере выполните команду:

```
C:\Users\<имя пользователя>\Desktop\KUMA>kuma.exe agent --id <Kaspersky SIEM Cloud agent service ID> --
uninstall
```

8 Проверка поступления событий DNS-сервера в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка получения событий DNS-сервера с помощью коннектора ETW выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Microsoft 365

Вы можете настроить получение событий из облачного решения Microsoft 365 (Office 365) в Kaspersky SIEM Cloud.

Настройка получения событий состоит из следующих этапов:

1 Настройка доступа к интерфейсам API управления Office 365 стандартными методами Microsoft

Для получения событий в Kaspersky SIEM Cloud выдайте необходимый набор разрешений API:

- **Microsoft.Graph**
- **Directory.Read.All**
- **API управления Office 365**
- **ActivityFeed.Read**
- **ActivityFeed.Read.Dlp**

2. Создание коллектора Kaspersky SIEM Cloud для получения событий Microsoft 365

При создании коллектора в веб-консоли на шаге **Транспорт** укажите тип коннектора **office365**, и на шаге **Парсинг событий** укажите нормализатор **[OOTB] Microsoft Office 365 json**.

3. Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Microsoft 365 требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

4. Проверка поступления событий Microsoft 365 в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий Microsoft 365 выполнена правильно, выполнив поиск связанных событий.

Unix и Linux

В этом разделе описана настройка получения событий с серверов и систем Linux и Unix, включая аудит, службы аутентификации и веб-серверы.

Auditd

Настройка получения событий Auditd на устройствах Linux состоит из следующих этапов:

1. Создание коллектора Kaspersky SIEM Cloud для получения событий Auditd

Для получения событий Auditd при создании коллектора на шаге **Транспорт** выберите тип коннектора **TCP** или **UDP** и переведите переключатель **Auditd** в активное положение.

2. Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Auditd требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

3. Настройка сервера источника событий

Вы можете настроить сервер источника событий с помощью одного из следующих сервисов:

rsyslog

Для передачи событий от сервера в коллектор Kaspersky SIEM Cloud используется сервис rsyslog.

Чтобы настроить передачу событий от сервера в коллектор:

1. Проверьте, что на сервере источнике событий установлен сервис rsyslog. Для этого выполните следующую команду:

   ```
   systemctl status rsyslog.service
   ```

   Если сервис rsyslog не установлен на сервере, установите его, выполнив следующую команду:

   ```
   yum install rsyslog
   systemctl enable rsyslog.service
   systemctl start rsyslog.service
   ```

2. Откройте файл сервиса audit.service /etc/audit/auditd.conf и измените значения следующих параметров:

   ```
   name_format=NONE
   log_format=ENRICHED
   ```

   Параметр `log_format` определяет формат записей, создаваемых сервисом auditd, и должен иметь значение `ENRICHED`, чтобы в событиях сохранялась информация о пользователях.

   После изменения параметров перезапустите сервис auditd с помощью команды:

   ```
   sudo systemctl restart auditd.service
   ```

3. В папке `/etc/rsyslog.d` создайте файл audit.conf со следующим содержанием в зависимости от используемого протокола:

   - Для отправки событий по протоколу TCP:

     ```
     $ModLoad imfile
     $InputFileName /var/log/audit/audit.log
     $InputFileTag tag_audit_log:
     $InputFileStateFile audit_log
     $InputFileSeverity info
     $InputFileFacility local6
     $InputRunFileMonitor
     *.* @@<IP-Kaspersky SIEM Cloud collector address>:<Kaspersky SIEM Cloud collector port>
     ```

     Например:

     ```
     *.* @@192.1.3.4:5858
     ```

- Для отправки событий по протоколу UDP:

```
$ModLoad imfile
$InputFileName /var/log/audit/audit.log
$InputFileTag tag_audit_log:
$InputFileStateFile audit_log
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor
template(name="AuditFormat" type="string" string="<%PRI%>%TIMESTAMP:::date-rfc3339% %HOSTNAME% %syslogtag%
%msg%")
*.* @<IP-Kaspersky SIEM Cloud collector address>:<Kaspersky SIEM Cloud collector port>
```

Например

```
*.* @192.1.3.4:5858;AuditFormat
```

4. Сохраните изменения в файле `audit.conf`.

5. Перезапустите сервис rsyslog, выполнив следующую команду:

```
systemctl restart rsyslog.service
```

Сервер источника событий настроен. Данные о событиях передаются с сервера в коллектор Kaspersky SIEM Cloud.

syslog-ng

Для передачи событий от сервера в коллектор Kaspersky SIEM Cloud используется сервис syslog-ng.

Чтобы настроить передачу событий от сервера в коллектор:

1. Проверьте, что на сервере-источнике событий установлен сервис syslog-ng, выполнив следующую команду:

   ```
   systemctl status syslog-ng.service
   ```

   Если сервис syslog-ng не установлен на сервере, установите его, выполнив команду в соответствии с вашей системой управления пакетами:

   APT (Debian, Ubuntu)

   ```
   apt install syslog-ng
   ```

   YUM (CentOS 7, RHEL):

   ```
   yum install syslog-ng
   ```

   DNF (Fedora, CentOS 8)

   ```
   dnf install syslog-ng
   ```

   Zypper (openSUSE)

   ```
   zypper install syslog-ng
   ```

   Pacman (Arch Linux)

   ```
   pacman -S syslog-ng
   ```

   Snap (если доступно)

   ```
   snap install syslog-ng
   ```

2. После установки запустите сервис syslog-ng:

   ```
   systemctl enable syslog-ng.service
   systemctl start syslog-ng.service
   ```

3. Откройте файл параметров /etc/audit/auditd.conf сервиса audit.service и измените значение параметра `name_format`, присвоив этому параметру значение `NONE`:

   ```
   name_format=NONE
   ```

4. После изменения параметра перезапустите сервис auditd с помощью команды:

   ```
   sudo systemctl restart auditd.service
   ```

5. В папке `/etc/syslog-ng создайте файл audit.conf` со следующим содержанием в зависимости от используемого протокола:

Для отправки событий по протоколу TCP

```
source s_audit_log {
file("/var/log/audit/audit.log"
persist-name("s_audit_log_for_siem")
follow-freq(1)
program-override("auditd:")
flags(no-parse));
};
log {
source(s_audit_log);
destination(d_audit_log);
};
# Форматирование сообщений
template AuditFormat {
template("<${PRI}>${ISODATE} ${HOST} ${MSG}\n");
};
# Передача журналов аудита на указанный адрес коллектора Kaspersky SIEM Cloud
destination d_audit_log {
tcp("<IP-адрес коллектора Kaspersky SIEM Cloud>" port(<порт коллектора Kaspersky SIEM Cloud>) persist-
name("collector-audit") template(AuditFormat));
};
```

Для отправки событий по протоколу UDP

```
source s_audit_log {
file("/var/log/audit/audit.log"
persist-name("s_audit_log_for_siem")
follow-freq(1)
program-override("auditd:")
flags(no-parse));
};
log {
source(s_audit_log);
destination(d_audit_log);
};
# Форматирование сообщений
template AuditFormat {
template("<${PRI}>${ISODATE} ${HOST} ${MSG}");
};
# Передача журналов аудита на указанный адрес коллектора Kaspersky SIEM Cloud
destination d_audit_log {
udp("<IP-адрес коллектора Kaspersky SIEM Cloud>" port(<порт коллектора Kaspersky SIEM Cloud>) persist-
name("collector-audit") template(AuditFormat));
};
```

6. Сохраните изменения в файле `audit.conf`.

7. Добавьте в конфигурационный файл `/etc/syslog-ng/syslog-ng.conf` следующую строку:

```
@include " audit.conf "
```

8. Перезапустите сервис syslog-ng, выполнив следующую команду:

```
systemctl restart syslog-ng.service
```

Сервер источника событий настроен. Данные о событиях передаются с сервера в коллектор Kaspersky SIEM Cloud.

4 Проверка поступления событий Auditd в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий Auditd выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

FreeIPA

Настройка получения событий FreeIPA в Kaspersky SIEM Cloud по протоколу Syslog состоит из следующих этапов:

1 Настройка передачи событий FreeIPA в Kaspersky SIEM Cloud

1. Подключитесь к серверу FreeIPA по протоколу SSH под учетной записью с правами администратора.
2. В директории `/etc/rsyslog.d/` создайте файл `freeipa-to-siem.conf`.
3. В конфигурационный файл `/etc/rsyslog.d/freeipa-to-siem.conf` добавьте следующие строки:

```
$ModLoad imfile
input(type="imfile"
      File="/var/log/httpd/error_log"
      Tag="tag_FreeIPA_log_httpd"
      facility="local3")
input(type="imfile"
      File="/var/log/dirsrv/slapd-*/audit"
      Tag="tag_FreeIPA_log_audit"
      StartMsg.regex="^time:"
      facility="local3")
input(type="imfile"
      File="/var/log/dirsrv/slapd-*/errors"
      Tag="tag_FreeIPA_log_errors"
      facility="local3")
input(type="imfile"
      File="/var/log/dirsrv/slapd-*/access"
      Tag="tag_FreeIPA_log_access"
      facility="local3")
input(type="imfile"
      File="/var/log/krb5kdc.log"
      Tag="tag_FreeIPA_log_krb5kdc"
      facility="local3")

template(name="ls_json" type="list" option.json="on") {
    constant(value="{")
    constant(value="\"@timestamp\":\"") property(name="timegenerated" dateFormat="rfc3339")
    constant(value="\",\"@version\":\"1")
    constant(value="\",\"message\":\"") property(name="msg")
    constant(value="\",\"host\":\"") property(name="fromhost")
    constant(value="\",\"host_ip\":\"") property(name="fromhost-ip")
    constant(value="\",\"logsource\":\"") property(name="fromhost")
    constant(value="\",\"severity_label\":\"") property(name="syslogseverity-text")
    constant(value="\",\"severity\":\"") property(name="syslogseverity")
    constant(value="\",\"facility_label\":\"") property(name="syslogfacility-text")
    constant(value="\",\"facility\":\"") property(name="syslogfacility")
    constant(value="\",\"program\":\"") property(name="programname")
    constant(value="\",\"pid\":\"") property(name="procid")
    constant(value="\",\"syslogtag\":\"") property(name="syslogtag")
    constant(value="\"}\n")
}

if $syslogtag contains 'tag_FreeIPA_log' then {
    action(type="omfwd"
           target="<Kaspersky SIEM Cloud collector IP address>"
           port="<Kaspersky SIEM Cloud collector port>"
           protocol="<udp or tcp>"
           template="ls_json")
    stop
}
```

4. В конфигурационный файл `/etc/rsyslog.conf` добавьте следующие строки:

```
$IncludeConfig /etc/rsyslog.d/freeipa-to-siem.conf
$RepeatedMsgReduction off
```

5. При необходимости выключите локальную запись событий FreeIPA, выполнив следующие действия:

   a. Откройте на редактирование конфигурационный файл `rsyslog /etc/rsyslog.conf` или файл правил по умолчанию `/etc/rsyslog.d/50-default.conf`.

   b. Найдите в файле строку, отвечающую за запись системных событий, и добавьте в нее параметр `local3.none`, так как в конфигурационном файле `/etc/rsyslog.d/freeipa-to-siem.conf` параметру `facility` присвоено значение `local3`. Измененная строка должна выглядеть следующим образом:

   ```
   *.info;mail.none;authpriv.none;cron.none;local3.none    /var/log/messages
   ```

   Если значение параметра `facility local3` уже используется другой программой на сервере, измените значение параметра `facility` для FreeIPA в файле `/etc/rsyslog.d/freeipa-to-siem.conf` на другое значение и внесите соответствующие правки в выбранном конфигурационном файле `rsyslog`.

   c. Сохраните изменения.

6. Сохраните изменения в конфигурационном файле `/etc/rsyslog.d/freeipa-to-siem.conf`.

7. Перезапустите сервис rsyslog, выполнив следующую команду:

```
sudo systemctl restart rsyslog.service
```

❷ Создание коллектора Kaspersky SIEM Cloud для получения событий FreeIPA

Для получения событий FreeIPA при создании коллектора Kaspersky SIEM Cloud на шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] FreeIPA**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий FreeIPA требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Проверка поступления событий FreeIPA в Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий FreeIPA выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

FreeRADIUS

Вы можете настроить получение событий программы FreeRADIUS версии 3.0.26 в Kaspersky SIEM Cloud.

Настройка получения событий состоит из следующих этапов:

1 Настройка аудита событий FreeRADIUS

1. Подключитесь к серверу, на котором установлена система FreeRADIUS, под учетной записью с правами администратора.
2. Создайте резервную копию конфигурационного файла FreeRADIUS с помощью команды:

```
sudo cp /etc/freeradius/3.0/radiusd.conf /etc/freeradius /3.0/radiusd.conf.bak
```

3. Откройте конфигурационный файл FreeRADIUS для редактирования с помощью команды:

```
sudo nano /etc/freeradius/3.0/radiusd.conf
```

4. В секции log измените параметры следующим образом:

```
destination = syslog
syslog_facility = daemon
stripped_names = no
auth = yes
auth_badpass = yes
auth_goodpass = yes
```

5. Сохраните конфигурационный файл.

Аудит событий FreeRADIUS будет настроен.

2 Настройка Syslog-сервера для отправки событий FreeRADIUS

Для передачи событий от сервера FreeRADIUS в коллектор Kaspersky SIEM Cloud используется сервис rsyslog.

1. В директории `/etc/rsyslog.d/` создайте файл `FreeRADIUS-to-siem.conf` и добавьте в него следующую строку:

```
If $programname contains 'radiusd' then @<collector IP address>:<collector port>
```

Если вы хотите отправлять события по протоколу TCP, содержимое файла должно быть таким:

```
If $programname contains 'radiusd' then @@<collector IP address>:<collector port>
```

2. Создайте резервную копию файла `/etc/rsyslog.conf`.
3. В конфигурационный файл `/etc/rsyslog.conf` добавьте следующие строки:

```
$IncludeConfig /etc/FreeRADIUS-to-siem.conf
$RepeatedMsgReduction off
```

4. Сохраните внесенные изменения.

5. Перезапустите службу rsyslog, выполнив следующую команду:

```
sudo systemctl restart rsyslog.service
```

Передача событий от сервера FreeRADIUS в коллектор Kaspersky SIEM Cloud будет настроена.

❸ Создание коллектора Kaspersky SIEM Cloud для получения событий FreeRADIUS

Для получения событий FreeRADIUS при создании коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] FreeRADIUS syslog**, на шаге **Транспорт** выберите тип коннектора **tcp** или **udp**.

❹ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий FreeRADIUS требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❺ Проверка поступления событий FreeRADIUS в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий FreeRADIUS выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

ProFTPD

Kaspersky SIEM Cloud позволяет осуществлять мониторинг событий ProFTPD на устройствах с операционной системой Linux. Сбор и аудит событий выполняются средствами ProFTPD, после чего события передаются в Kaspersky SIEM Cloud через syslog-сервер rsyslog.

Настройка получения событий ProFTPD состоит из следующих этапов:

❶ Настройка аудита событий ProFTPD

1. Создайте резервную копию конфигурационного файла `/etc/proftpd/proftpd.conf`.

2. Откройте файл `proftpd.conf` и добавьте или измените значения следующих параметров:

```
LogFormat default "%t %a %A %b %F %H %h %l %u \"%r\" %s %{file-modified} %{gid} %{transfer-status}"
LogFormat auth "%t %a %A %b %F %H %h %l %u \"%r\" %s %{file-modified} %{gid} %{transfer-status}"
ExtendedLog /var/log/proftpd/access.log ALL default
ExtendedLog /var/log/proftpd/auth.log AUTH auth
```

3. Сохраните изменения и перезапустите сервис, выполнив команду:

```
sudo systemctl restart proftpd
```

Аудит событий ProFTPD будет настроен.

Система ProFTPD не выполняет ротацию журналов. Чтобы снизить риск переполнения дискового пространства, рекомендуется использовать внешние инструменты ротации журналов, например Logrotate или Logadm

❷ Создание коллектора Kaspersky SIEM Cloud для событий ProFTPD

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Транспорт** нужно указать порт и протокол, которые используются при настройке syslog-сервера для отправки событий. Для получения событий аудита из ProFTPD на шаге **Парсинг событий** нужно выбрать нормализатор **[OOTB] Proftpd syslog**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий ProFTPD требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Настройка syslog-сервера для отправки событий

Для передачи событий от сервера в коллектор Kaspersky SIEM Cloud используется сервис rsyslog.

1. Проверьте, что на сервере источника событий установлен сервис rsyslog. Для этого выполните следующую команду:

   ```
   systemctl status rsyslog.service
   ```

   Если сервис rsyslog не установлен на сервере, установите его, выполнив следующие команды:

   ```
   yum install rsyslog
   systemctl enable rsyslog.service
   systemctl start rsyslog.service
   ```

2. В директории /etc/rsyslog.d создайте файл proftpd.conf со следующим содержанием в зависимости от используемого протокола:

   - Для отправки событий по протоколу TCP:

     ```
     $ModLoad imfile
     $InputFileName /var/log/proftpd/*.log
     $InputFileTag tag_proftpd_log:
     $InputFileStateFile proftpd_log
     $InputRunFileMonitor
     if $syslogtag contains 'tag_proftpd_log' then {
     *.* action(type="omfwd" target="@<Kaspersky SIEM Cloud collector IP address>" port="<Kaspersky SIEM Cloud
     collector port>" protocol="tcp")
         stop
     }
     ```

   - Для отправки событий по протоколу UDP:

     ```
     $ModLoad imfile
     $InputFileName /var/log/proftpd/*.log
     $InputFileTag tag_proftpd_log:
     $InputFileStateFile proftpd_log
     $InputRunFileMonitor
     if $syslogtag contains 'tag_proftpd_log' then {
     *.* action(type="omfwd" target="@<Kaspersky SIEM Cloud collector IP address>" port="<Kaspersky SIEM Cloud
     collector port>" protocol="udp")
         stop
     }
     ```

3. Сохраните изменения в файле `proftpd.conf`.

4. Перезапустите сервис rsyslog, выполнив следующую команду:

```
systemctl restart rsyslog.service
```

Сервер источника событий настроен. Данные о событиях будут передаваться с сервера в коллектор Kaspersky SIEM Cloud.

❺ Проверка поступления событий ProFTPD в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка поступления событий из ProFTPD выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Vsftpd

Kaspersky SIEM Cloud позволяет осуществлять мониторинг событий Vsftpd на устройствах с операционной системой Linux. Сбор и аудит событий выполняются средствами Vsftpd, после чего события передаются в Kaspersky SIEM Cloud через syslog-сервер rsyslog.

Настройка получения событий Vsftpd состоит из следующих этапов:

❶ Настройка аудита событий Vsftpd

1. Создайте резервную копию конфигурационного файла `/etc/vsftpd/vsftpd.conf`.

2. Откройте файл `vsftpd.conf` и добавьте или измените значения следующих параметров:

```
xferlog_enable=YES
xferlog_std_format=NO
xferlog_file=/var/log/vsftpd.log
log_ftp_protocol=YES
```

3. Сохраните изменения и перезапустите сервис, выполнив команду:

```
sudo systemctl restart vsftpd
```

Аудит событий Vsftpd будет настроен.

Система Vsftpd не выполняет ротацию журналов. Чтобы снизить риск переполнения дискового пространства, рекомендуется использовать внешние инструменты ротации журналов, например Logrotate или Logadm.

❷ Создание коллектора Kaspersky SIEM Cloud для событий Vsftpd

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Транспорт** нужно указать порт и протокол, которые используются при настройке syslog-сервера для отправки событий. Для получения событий аудита из Vsftpd на шаге **Парсинг событий** нужно выбрать нормализатор **[OOTB] Vsftpd syslog**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Vsftpd требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Настройка syslog-сервера для отправки событий

Для передачи событий от сервера в коллектор Kaspersky SIEM Cloud используется сервис rsyslog.

1. Проверьте, что на сервере источника событий установлен сервис rsyslog. Для этого выполните следующую команду:

   ```
   systemctl status rsyslog.service
   ```

   Если сервис rsyslog не установлен на сервере, установите его, выполнив следующие команды:

   ```
   yum install rsyslog
   systemctl enable rsyslog.service
   systemctl start rsyslog.service
   ```

2. В директории `/etc/rsyslog.d` создайте файл `vsftpd.conf` со следующим содержанием в зависимости от используемого протокола:

   - Для отправки событий по протоколу TCP:

     ```
     $ModLoad imfile
     $InputFileName /var/log/vsftpd.log
     $InputFileTag tag_vsftpd_log:
     $InputFileStateFile vsftpd_log
     $InputRunFileMonitor
     *.* @@<IKaspersky SIEM Cloud collector IP address>:<Kaspersky SIEM Cloud collector port>
     ```

     Пример

     ```
     *.* @@192.1.3.4:5858
     ```

   - Для отправки событий по протоколу UDP:

     ```
     $ModLoad imfile
     $InputFileName /var/log/vsftpd.log
     $InputFileTag tag_vsftpd_log:
     $InputFileStateFile vsftpd_log
     $InputRunFileMonitor
     *.* @<Kaspersky SIEM Cloud collector IP address>:<Kaspersky SIEM Cloud collector port>
     ```

     Пример

     ```
     *.* @192.1.3.4:5858
     ```

3. Сохраните изменения в файле `vsftpd.conf`.

4. Перезапустите сервис rsyslog, выполнив следующую команду:

```
systemctl restart rsyslog.service
```

Сервер источника событий будет настроен. Данные о событиях будут передаваться с сервера в коллектор Kaspersky SIEM Cloud.

❺ Проверка поступления событий Vsftpd в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка поступления событий из Vsftpd выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

HAProxy

Kaspersky SIEM Cloud позволяет осуществлять мониторинг событий балансировщика нагрузки HAProxy (версия 2.4) в форматах HTTP, TCP, HTTP CLF, Default, HTTPS (для версии 2.6 и выше), TCP CLF (для версии 3.2 и выше), поступающих по протоколу syslog.

Настройка получения событий HAProxy состоит из следующих этапов:

❶ Настройка передачи событий HAProxy

1. Проверьте синтаксис в конфигурационном файле на наличие ошибок, выполнив команду:

```
haproxy -c -V -f /etc/haproxy/haproxy.cfg
```

Возможные сообщения при проверке конфигурационного файла

Если в конфигурационном файле синтаксические ошибки отсутствуют, HAProxy отобразит уведомление `Configuration file is valid`.

Если в конфигурационном файле найдены синтаксические ошибки, HAProxy сообщит, в чем заключается ошибка, например:

`[NOTICE] (284146): haproxy version is 2.4.24-0ubuntu0.22.04.2`

`[NOTICE] (284146): path to executable is /usr/sbin/haproxy`

`[ALERT] (284146): parsing [/etc/haproxy/haproxy.cfg:25] : unknown option 'httpdlog'; did you mean 'httplog' maybe ?`

`[ALERT] (284146): Error(s) found in configuration file : /etc/haproxy/haproxy.cfg`

`[ALERT] (284146): Fatal errors found in configuration`

Подробнее о синтаксисе конфигурационного файла см. в официальной документации HAProxy.

2. Если проверка синтаксиса прошла успешно, выполните резервное копирование исходного конфигурационного файла с помощью следующей команды:

```
sudo cp /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy_backup.cfg
```

3. Откройте конфигурационный файл `haproxy.cfg`, выполнив следующую команду:

```
sudo vi /etc/haproxy/haproxy.cfg
```

Дальнейшие шаги инструкции предполагают, что для всех групп серверов применяются единые параметры записи в журнал. В этом случае параметры записи в журнал указываются в секции `global`, а в секции `defaults` используется строка `log global`.

Если требуется более детальная настройка записи в журнал, нужно удалить строку `log global` из секции `defaults`. Так как секции `frontend`, `backend` и `listen` по умолчанию наследуют параметры из секции `defaults`, это приведет к выключению глобальной записи в журнал. В таком случае необходимо определить параметры записи в журнал в каждой секции, добавив строку следующего вида:

```
log <IP_адрес_коллектора_Kaspersky SIEM Cloud> [len <length_in_bytes>] [format <syslog_message_format>] [sample
<ranges>:<sample_size>] <facility> [<level> [<minimum_level>]]
```

4. В секции `global` укажите IP-адрес коллектора Kaspersky SIEM Cloud:

```
log <collector_IP_address>:<port>
```

5. В секции `global` добавьте следующую строку для добавления имени хоста в заголовок syslog:

```
log-send-hostname <host_name>
```

6. В секции `defaults` добавьте строку для использования глобальных параметров записи в журнал:

```
log global
```

7. В секции `defaults` укажите формат журналирования:

- Для балансировщиков 4 уровня (TCP):

```
option tcplog
```

Пример секции defaults с настроенными параметрами

```
defaults
log global
mode tcp
option tcplog
option dontlognull
timeout connect 5000
timeout client 50000
timeout server 50000
errorfile 400 /etc/haproxy/errors/400.http
errorfile 403 /etc/haproxy/errors/403.http
errorfile 408 /etc/haproxy/errors/408.http
errorfile 500 /etc/haproxy/errors/500.http
errorfile 502 /etc/haproxy/errors/502.http
errorfile 503 /etc/haproxy/errors/503.http
errorfile 504 /etc/haproxy/errors/504.http
```

- Для балансировщиков 7 уровня (HTTP):

```
option httplog
```

Пример секции defaults с настроенными параметрами

```
defaults
log global
mode http
option httplog
option dontlognull
timeout connect 5000
timeout client 50000
timeout server 50000
errorfile 400 /etc/haproxy/errors/400.http
errorfile 403 /etc/haproxy/errors/403.http
errorfile 408 /etc/haproxy/errors/408.http
errorfile 500 /etc/haproxy/errors/500.http
errorfile 502 /etc/haproxy/errors/502.http
errorfile 503 /etc/haproxy/errors/503.http
errorfile 504 /etc/haproxy/errors/504.http
```

8. Если требуется включить запись в журнал HTTP-заголовков запроса, добавьте в секцию `frontend` или `listen` строку:

```
capture request header <header_name> len <header_length_in_bytes>
```

Каждый заголовок необходимо указывать отдельной строкой, например:

```
capture request header User-agent len 50
capture request header Host len 30
capture request header X-Forwarded-For len 15
```

9. Если требуется включить запись в журнал HTTP-заголовков ответа, добавьте в секцию `frontend` или `listen` строку:

```
capture response header <header_name> len <header_length_in_bytes>
```

Каждый заголовок необходимо указывать отдельной строкой, например:

```
capture response header User-agent len 50
capture response header Host len 30
capture response header X-Forwarded-For len 15
```

10. Если требуется включить запись в журнал HTTP-cookie, добавьте в секцию `frontend` или `listen` строку:

```
capture cookie <cookie_name> len <cookie_size_in_bytes>
```

В журнал записывается только первый файл cookie с указанным именем.

11. Проверьте синтаксис в конфигурационном файле на наличие ошибок, выполнив команду (см. пункт 1 инструкции):

```
haproxy -c -V -f /etc/haproxy/haproxy.cfg
```

12. Перезагрузите конфигурацию, выполнив следующую команду:

```
sudo systemctl reload haproxy
```

13. Проверьте, что балансировщик нагрузки HAProxy запущен и работает правильно, выполнив следующую команду:

```
sudo systemctl status haproxy
```

Передача событий из HAProxy будет настроена.

❷ Создание коллектора Kaspersky SIEM Cloud для получения событий HAProxy

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Парсинг событий** нужно выбрать нормализатор **[OOTB] HAProxy syslog**, а на шаге **Транспорт** нужно выбрать тип коннектора **udp**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий HAProxy требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Проверка поступления событий HAProxy в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что поступление событий из HAProxy настроено правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Apache Tomcat

Kaspersky SIEM Cloud позволяет осуществлять мониторинг событий аудита веб-сервера Apache Tomcat версий 9.0 и выше, 10.1 и выше и 11.0 и выше, развернутого на устройствах с операционной системой Linux. Сбор и аудит событий выполняются средствами Apache Tomcat, после чего события передаются в Kaspersky SIEM Cloud через syslog-сервер rsyslog.

Настройка получения событий Apache Tomcat состоит из следующих этапов:

❶ Настройка аудита событий Apache Tomcat

1. Подключитесь по протоколу SSH к серверу Apache Tomcat под учетной записью с правами администратора.

   Дальнейшие шаги инструкции предполагают, что на сервере настроены стандартные переменные среды `$CATALINA_HOME` и `$JAVA_HOME`.

   Подробнее о переменных см. в руководстве по установке Apache Tomcat.

2. Выполните резервное копирование исходного конфигурационного файла с помощью команды:

```
sudo cp $CATALINA_HOME/conf/server.xml $CATALINA_HOME/conf/server_backup.xml
```

3. Откройте конфигурационный файл Apache Tomcat с помощью команды:

```
sudo vi $CATALINA_HOME/conf/server.xml
```

4. Найдите элемент `<Valve className="org.apache.catalina.valves.AccessLogValve" ... />` и замените его на следующий вариант с использованием `JsonAccessLogValve`:

```
<Valve className="org.apache.catalina.valves.JsonAccessLogValve" directory="logs"
prefix="access_log" suffix=".txt"
maxDays="7"
pattern="%h %a %t %m %U %q %r %H %A %v %p %s %b %X %I %{User-Agent}i %{Cookie}c"/>
```

Если невозможно использовать `JsonAccessLogValve`, оставьте `AccessLogValve`, но задайте расширенный шаблон, чтобы увеличить объем собираемых полей:

```
pattern="host=%h|remoteAddr=%a|time=%t|method=%m|path=%U|query=%q|request=%r|protocol=%H|localAddr=%A|localServerN
Agent=%{User-Agent}i|Cookie=%{Cookie}c"
```

Пример конфигурации с AccessLogValve:

```
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="access_log" suffix=".txt"
maxDays="7"
pattern="host=%h|remoteAddr=%a|time=%t|method=%m|path=%U|query=%q|request=%r|protocol=%H|localAddr=%A|localServerN
Agent=%{User-Agent}i|Cookie=%{Cookie}c"/>
```

Нормализатор также поддерживает шаблоны Common и Combined для `AccessLogValve` и `JsonAccessLogValve`.

5. Перезапустите веб-сервер Apache Tomcat с помощью следующих команд:

```
sudo $CATALINA_HOME/bin/shutdown.sh
sudo $CATALINA_HOME/bin/startup.sh
sudo systemctl restart tomcat.service
```

Аудит событий Apache Tomcat будет настроен.

❷ Создание коллектора Kaspersky SIEM Cloud для событий Apache Tomcat

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Парсинг событий** нужно выбрать нормализатор **[OOTB] Apache Tomcat**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Apache Tomcat требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

4 Настройка syslog-сервера для отправки событий

Для передачи событий от сервера в коллектор Kaspersky SIEM Cloud используется сервис rsyslog.

1. Проверьте, что на сервере, являющимся источником событий, установлен сервис rsyslog. Для этого выполните следующую команду:

   ```
   systemctl status rsyslog.service
   ```

   Если сервис запущен, то отобразится уведомление следующего вида:

   ```
   Active: active (running) since Tue 2025-09-23 15:31:30 MSK; 1 week 0 days ago
   ```

   Если сервис rsyslog не установлен на сервере, установите его, выполнив следующие команды:

   ```
   sudo apt install rsyslog
   sudo systemctl enable rsyslog.service
   sudo systemctl start rsyslog.service
   ```

2. Проверьте синтаксис в конфигурационном файле с помощью следующей команды:

   ```
   rsyslogd -N1
   ```

   Возможные сообщения при проверке конфигурационного файла

   Если в конфигурационном файле синтаксические ошибки отсутствуют, сервис rsyslog отобразит следующие уведомления:

   ```
   rsyslogd: version 8.2112.0, config validation run (level 1), master config
   /etc/rsyslog.conf
   rsyslogd: End of config validation run. Bye.
   ```

   Если в конфигурационном файле найдены синтаксические ошибки, сервис rsyslog сообщит, в чем заключается ошибка, например:

   ```
   rsyslogd: version 8.2112.0, config validation run (level 1), master config
   /etc/rsyslog.conf
   rsyslogd: module 'imfile' already in this config, cannot be added  [v8.2112.0 try
   https://www.rsyslog.com/e/2221 ]
   rsyslogd: module 'imfile' already in this config, cannot be added  [v8.2112.0 try
   https://www.rsyslog.com/e/2221 ]
   rsyslogd: parameter "maxLinesAtOnce" not permited in inotify mode - ignored [v8.2112.0
   try https://www.rsyslog.com/e/2222 ]
   rsyslogd: $WorkDirectory: /var/lib/rsyslog not a directory - directive ignored
   [v8.2112.0 try https://www.rsyslog.com/e/2181 ]
   rsyslogd: imfile: no working or state file directory set, imfile will create state
   files in the current working directory (probably the root dir). Use
   global(workDirectory="/some/path") to set the working directory [v8.2112.0 try
   https://www.rsyslog.com/e/2450]
   ```

3. Откройте конфигурационный файл `rsyslog.conf`, выполнив следующую команду:

   ```
   sudo vi /etc/rsyslog.conf
   ```

4. Проверьте, что в файле указана строка, разрешающая загрузку конфигураций из директории `/etc/rsyslog.d`, выполнив следующие команды

```
# Include all config files in /etc/rsyslog.d/
include(file="/etc/rsyslog.d/*.conf" mode="optional")
```

5. Создайте конфигурационный файл `apache_tomcat_to_siem.conf` в директории `/etc/rsyslog.d/` с помощью следующей команды:

```
sudo touch /etc/rsyslog.d/apache_tomcat_to_siem.conf
```

6. Откройте созданный конфигурационный файл `apache_tomcat_to_siem.conf` с помощью следующей команды:

```
sudo vi /etc/rsyslog.d/apache_tomcat_to_siem.conf
```

7. Выполните следующую команду, чтобы узнать абсолютный путь к директории Apache Tomcat:

```
printenv CATALINA_HOME
```

Абсолютный путь нужен для того, чтобы указать его в конфигурационном файле, так как сервис rsyslog не поддерживает использование переменных окружения.

8. Добавьте в конфигурационный файл правила для чтения `Access Log` и пересылки данных на коллектор Kaspersky SIEM Cloud:

```
input(
        type="imfile"
        File="<absolute_path_from_step 7>/logs/access_log*.txt"
        Tag="apachetomcat"
)

if $programname == "apachetomcat" then {
        action(
                type="omfwd"
                target="<Kaspersky SIEM Cloud_collector_FQDN_or_IP_address>"
                port="<Kaspersky SIEM Cloud_collector_port>"
                protocol="<udp_or_tcp>"
        )
}
```

9. Проверьте синтаксис в конфигурационном файле на наличие ошибок с помощью следующей команды (см. пункт 2 инструкции):

```
rsyslogd -N1
```

10. Перезагрузите сервис rsyslog с помощью команды:

```
sudo systemctl restart rsyslog
```

11. Проверьте, что сервис rsyslog запущен и работает правильно, выполнив следующую команду:

```
sudo systemctl status rsyslog
```

Передача событий от сервера, на котором установлена система Apache Tomcat, в коллектор будет настроена.

5 Проверка поступления событий Apache Tomcat в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка поступления событий из Apache Tomcat выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Сетевые и защитные устройства

В этом разделе описана настройка получения событий с сетевых устройств и систем защиты.

ИВК Кольчуга-К

Вы можете настроить получение событий системы ИВК Кольчуга-К в Kaspersky SIEM Cloud.

Настройка получения событий состоит из следующих этапов:

1 Настройка передачи событий ИВК Кольчуга-К в Kaspersky SIEM Cloud

1. Подключитесь к межсетевому экрану с правами администратора по протоколу SSH.
2. Создайте резервную копию файлов `/etc/services` и `/etc/syslog.conf`.
3. В конфигурационном файле `/etc/syslog.conf` укажите FQDN или IP-адрес коллектора Kaspersky SIEM Cloud, например:

   ```
   *.* @kuma.example.com
   ```

   или

   ```
   *.* @192.168.0.100
   ```

4. Сохраните изменения в конфигурационном файле `/etc/syslog.conf`.
5. В конфигурационном файле /etc/services укажите порт и протокол, который используется коллектором Kaspersky SIEM Cloud. Например:

   ```
   syslog          10514/udp
   ```

6. Сохраните изменения в конфигурационном файле `/etc/services`.

7. Перезапустите syslog-сервер межсетевого экрана с помощью команды:

```
service syslogd restart
```

❷ Создание коллектора Kaspersky SIEM Cloud для получения событий ИВК Кольчуга-К

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Парсинг событий** выберите нормализатор **[OOTB] Kolchuga-K syslog**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий ИВК Кольчуга-К требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Проверка поступления событий ИВК Кольчуга-К в Kaspersky SIEM Cloud

Вы можете проверить, что настройка источника событий ИВК Кольчуга-К выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

КриптоПро NGate

Вы можете настроить получение событий программы КриптоПро NGate в Kaspersky SIEM Cloud.

Настройка получения событий состоит из следующих этапов:

❶ Настройка передачи событий КриптоПро NGate в Kaspersky SIEM Cloud

1. Подключитесь к веб-интерфейсу системы управления NGate.
2. Подключите удаленные syslog-серверы к системе управления. Для этого выполните следующие действия:
   a. Откройте страницу списка syslog-серверов **External Services** → **Syslog Server** → **Add Syslog Server**.
   b. Введите параметры syslog-сервера и нажмите на значок ✔.
3. Привяжите syslog-серверы к конфигурации для записи журналов работы кластера. Для этого выполните следующие действия:
   a. В разделе **Clusters** → **Summary** выберите настраиваемый кластер.
   b. На вкладке **Configurations** нажмите на элемент **Configuration** нужного кластера для входа на страницу настроек конфигурации.
   c. В поле **Syslog Servers** настраиваемой конфигурации нажмите на кнопку **Assign**.
   d. Установите флажки для syslog-серверов, которые вы хотите привязать, и нажмите на значок ✔.
      Вы можете привязать неограниченное число серверов.
      Чтобы добавить новые syslog-серверы, нажмите на значок ✚.
   e. Опубликуйте конфигурацию для активации новых параметров.

4. Привяжите syslog-серверы
   к системе управления для записи журналов работы Администратора. Для этого выполните следующие действия:

   a. Выберите пункт меню **Management Center Settings** и на открывшейся странице в блоке **Syslog servers** нажмите на кнопку **Assign**.

   b. В окне **Assign Syslog Servers to Management Center** установите флажок для тех syslog-серверов, которые вы хотите привязать, затем нажмите на значок .

   Вы можете привязать неограниченное количество серверов.

   События КриптоПро NGate будут передаваться в Kaspersky SIEM Cloud.

❷ Создание коллектора Kaspersky SIEM Cloud для получения событий КриптоПро NGate

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Парсинг событий** выберите нормализатор **[OOTB] NGate syslog**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий КриптоПро NGate требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Проверка поступления событий КриптоПро NGate в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий КриптоПро NGate выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Ideco UTM

Вы можете настроить получение событий программы Ideco UTM в Kaspersky SIEM Cloud по протоколу Syslog.

Настройка получения событий состоит из следующих этапов:

❶ Настройка передачи событий Ideco UTM в Kaspersky SIEM Cloud

1. Подключитесь к веб-интерфейсу Ideco UTM под учетной записью с правами администратора.
2. В меню **Пересылка системных сообщений** переведите переключатель **Syslog** в положение **включено**.
3. В параметре **IP-адрес** укажите IP-адрес коллектора Kaspersky SIEM Cloud.
4. В параметре **Порт** введите порт, который прослушивает коллектор Kaspersky SIEM Cloud.
5. Нажмите **Сохранить** для применения внесенных изменений.

   Передача событий в Ideco UTM в Kaspersky SIEM Cloud будет настроена.

❷ Создание коллектора Kaspersky SIEM Cloud для получения событий Ideco UTM

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Парсинг событий** выберите нормализатор **[OOTB] Ideco UTM syslog**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Ideco UTM требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Проверка поступления событий Ideco UTM в Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий Ideco UTM выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

McAfee Web Gateway

Настройка получения событий от системы McAfee Web Gateway (версия 7.8), поступающих по протоколу Syslog в формате CEF в Kaspersky SIEM Cloud, состоит из следующих этапов:

❶ Создание учетной записи в McAfee Web Gateway

Настройку передачи событий необходимо выполнять под учетной записью с правами администратора:

1. В веб-интерфейсе McAfee Web Gateway откройте раздел **Policy** → **Rule Sets**.
2. Нажмите на **Log Handler** в нижней части левой панели веб-интерфейса.
3. Найдите нужный набор правил, разверните **Default rule set** и выберите в нем вложенный набор правил **CEF Syslog**.

   Содержимое вложенного набора правил отобразится в панели конфигурации.
4. Включите правило **Send to Syslog**.
5. Нажмите **Save Changes**.
6. Настройте отправку данных журнала аудите по syslog. Для этого перейдите в раздел **Configuration** → **Appliances** → **Log File Manager** → **Settings**.
7. Выберите **Write audit log to syslog**.

8. Для отправки данных по syslog измените параметры syslog-сервера `rsyslog.conf`, выполнив следующие действия:

   a. Перейдите в раздел **Configuration** → **File Editor**.

   b. В дереве файлов выберите файл `rsyslog.conf`.

      Содержимое файла отобразится на панели конфигурации.

   c. Измените файл rsyslog.conf, заменив содержимое строки `*.info;mail.none;authpriv.none;cron.none /var/log/messages` на `*.info;daemon.!=info;mail.none;authpriv.none;cron.none -/var/log/messages`.

9. Настройте отправку данных на сервер syslog в зависимости от выбранного протокола, добавив в конец файла строку:

```
Для отправки данных по протоколу UDP
```

```
daemon.info @<syslog server address in x.x.x.x format>:<port number>
```

```
Для отправки данных по протоколу TCP, добавьте в конец файла строку:
```

```
daemon.info @@<syslog server address in x.x.x.x format>:<port number>
```

10. Нажмите **Save Changes**.

❷ Создание коллектора Kaspersky SIEM Cloud для получения событий **McAfee Web Gateway**

При создании коллектора в Kaspersky SIEM Cloud на шаге **Парсинг событий** выберите нормализатор **[OOTB] McAfee Web Gateway**, на шаге **Транспорт** выберите тип коннектора tcp или udp в соответствии с тем, что вы выбрали при настройке передачи событий McAfee Web Gateway.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для получения событий McAfee Web Gateway требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Проверка поступления событий из **McAfee Web Gateway** в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка поступления событий из McAfee Web Gateway выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky.

Positive Technologies Network Attack Discovery

Вы можете настроить получение событий из Positive Technologies Network Attack Discovery (далее PT NAD) в Kaspersky SIEM Cloud.

Настройка получения событий состоит из следующих этапов:

❶ Настройка модуля ptdpi-worker@notifier для передачи событий PT NAD в Kaspersky SIEM Cloud

Для включения отправки информации об обнаруженных угрозах информационной безопасности необходимо настроить модуль ptdpi-worker@notifier.

В многосерверной конфигурации инструкцию нужно выполнять на основном сервере.

1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:

   ```
   sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
   ```

2. В секции `General settings` раскомментируйте параметр `workers` и добавьте `notifier` в список его значений.

   Например

   ```
   workers: ad alert dns es hosts notifier
   ```

3. Добавьте в конец файла строку вида `notifier.yaml.nad_web_url: <URL веб-интерфейса PT NAD>`.

   Например

   ```
   notifier.yaml.nad_web_url: https://ptnad.example.com
   ```

   Модуль `ptdpi-worker@notifier` будет использовать указанный URL для формирования ссылок на карточки сессий и активностей при отправке сообщений.

4. Перезапустите сенсор:

   ```
   sudo ptdpictl restart-all
   ```

Модуль `ptdpi-worker@notifier` будет настроен.

❷ Настройка отправки syslog-сообщений с информацией об активностях, атаках и индикаторах компрометации

Параметры, перечисленные в инструкции ниже могут отсутствовать в конфигурационном файле. Если параметр отсутствует, вам нужно добавить его в файл самостоятельно.

В многосерверной конфигурации PT NAD настройка выполняется на основном сервере.

1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:

   ```
   sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
   ```

2. По умолчанию PT NAD отправляет данные об активностях на русском языке. Чтобы получать данные на английском языке, измените значение параметра `notifier.yaml.syslog_notifier.locale` на `en`.

   Например

   ```
   notifier.yaml.syslog_notifier.locale: en
   ```

3. В параметре `notifier.yaml.syslog_notifier.addresses` добавьте секцию с параметрами отправки событий в Kaspersky SIEM Cloud.

   Параметр `<Название подключения>` может состоять только из букв латинского алфавита, цифр и символа подчеркивания.

   В параметре `address` необходимо указать IP-адрес коллектора Kaspersky SIEM Cloud. Остальные параметры можно не указывать, в таком случае будут использоваться значения по умолчанию.

```
notifier.yaml.syslog_notifier.addresses:
  <Connection name>:
        address: <For sending to a remote server: User Datagram Protocol (UDP, default) or TCP, address, and
port; for a local connection: Unix domain socket>
        doc_types: [<Comma-separated message types (alert for attack information, detection for activities, and
reputation for information about indicators of compromise). All message types are sent by default>]
        facility: <Numeric value of the subject category>
        ident: <Software label>
  <Connection name>:
        ...
```

Пример настройки отправки syslog-сообщений с информацией об активностях, атаках и индикаторах компрометации, отправляемых на два удаленных сервера по протоколам TCP и UDP без записи в локальный журнал

```
notifier.yaml.syslog_notifier.addresses:
  remote1:
    address: tcp://198.51.100.1:1514
  remote2:
    address: udp://198.51.100.2:2514
```

4. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.

5. Перезапустите модуль ptdpi-worker@`notifier`:

```
sudo ptdpictl restart-worker notifier
```

Настройка отправки событий в Kaspersky SIEM Cloud по Syslog выполнена.

❸ Создание коллектора Kaspersky SIEM Cloud для получения событий PT NAD

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Парсинг событий** выберите нормализатор **[OOTB] PT NAD json**.

❹ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий PT NAD требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❺ Проверка поступления событий PT NAD в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий PT NAD выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Snort

Вы можете настроить получение событий программы Snort версии 3 в Kaspersky SIEM Cloud.

Настройка получения событий состоит из следующих этапов:

❶ Настройка журналирования событий Snort

Убедитесь, что на сервере, на котором запущен Snort, есть минимум 500 МБ свободного дискового пространства для сохранения одного журнала событий Snort.
По достижении объема журнала 500 МБ Snort автоматически создаст новый файл, в имени которого будет указано текущее время в формате unixtime.
Мы рекомендуем отслеживать заполнение дискового пространства.

1. Подключитесь к серверу, на котором установлен Snort, под учетной записью с правами администратора.

2. Измените конфигурационный файл Snort. Для этого в командном интерпретаторе выполните команду:

```
sudo vi /usr/local/etc/snort/snort.lua
В конфигурационном файле измените содержимое блока alert_json:
alert_json =
{
file = true,
limit = 500,
fields = 'seconds action class b64_data dir dst_addr dst_ap dst_port eth_dst eth_len \
eth_src eth_type gid icmp_code icmp_id icmp_seq icmp_type iface ip_id ip_len msg mpls \
pkt_gen pkt_len pkt_num priority proto rev rule service sid src_addr src_ap src_port \
target tcp_ack tcp_flags tcp_len tcp_seq tcp_win tos ttl udp_len vlan timestamp',
}
```

3. Для завершения настройки выполните следующую команду:

```
sudo /usr/local/bin/snort -c /usr/local/etc/snort/snort.lua -s 65535 -k none -l /var/log/snort -i <name of the
interface Snort listens on> -m 0x1b
```

События Snort будут записываться в файл `/var/log/snort/alert_json.txt`.

❷ Создание коллектора Kaspersky SIEM Cloud для получения событий Snort

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Парсинг событий** выберите нормализатор **[OOTB] Snort 3 json file**, на шаге **Транспорт** выберите тип коннектора **file**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Snort требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Проверка поступления событий Snort в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий Snort выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Suricata

Настройка получения событий от программы Suricata версии 7.0.1 в Kaspersky SIEM Cloud состоит из следующих этапов:

❶ Настройка передачи событий Suricata в Kaspersky SIEM Cloud

1. Подключитесь по протоколу SSH к серверу, обладающему административными учетными записями.
2. Создайте резервную копию файла `/etc/suricata/suricata.yaml`.

```
Установите в конфигурационном файле /etc/suricata/suricata.yaml в секции eve-log следующие значения:
- eve-log:
  enabled: yes
  filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
  filename: eve.json
```

3. Сохраните изменения в файле конфигурации `/etc/suricata/suricata.yaml`.

События Suricata будут записываться в файл `/usr/local/var/log/suricata/eve.json`.

Suricata не поддерживает ограничение размера файла с событиями `eve.json`. При необходимости вы можете контролировать размер журнала с помощью ротации. Например, для настройки ежечасной ротации журнала добавьте в конфигурационный файл следующие строки:

```
outputs:
  - eve-log:
    filename: eve-%Y-%m-%d-%H:%M.json
    rotate-interval: hour
```

❷ Создание коллектора Kaspersky SIEM Cloud для получения событий Suricata

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Парсинг событий** выберите нормализатор **[OOTB] Suricata json file**, на шаге **Транспорт** выберите тип коннектора **file**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Suricata требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Проверка поступления событий Suricata в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий Suricata выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

zVirt

Kaspersky SIEM Cloud позволяет осуществлять мониторинг событий системы zVirt (версии zVirt 3.1, 4.4, 4.5, 5.0, zVirt Max 1.2), поступающих по протоколу Syslog

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий zVirt в Kaspersky SIEM Cloud.
2. Создание коллектора Kaspersky SIEM Cloud для получения событий zVirt.

   Для получения событий zVirt в мастере установки коллектора Kaspersky SIEM Cloud на шаге "Транспорт" выберите тип коннектора **tcp** или **udp**. На шаге **Парсинг событий** выберите нормализатор **[OOTB] OrionSoft zVirt syslog**.
3. Установка коллектора Kaspersky SIEM Cloud для получения событий zVirt.
4. Проверка поступления событий zVirt в коллектор Kaspersky SIEM Cloud

   Вы можете проверить, что поступление событий из системы zVirt настроено правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Настройка передачи событий zVirt в Kaspersky SIEM Cloud

Настройку передачи событий необходимо выполнять под учетной записью с правами администратора.

В системе zVirt можно настроить отправку сообщений о событиях как отдельных хостов, так и всех хостов отдельного кластера. Настройка журналирования отдельного хоста имеет наибольший приоритет над настройками журналирования кластера. При вводе хоста в новый кластер, его настройки передачи событий будут заменены на настройки кластера.

Чтобы настроить передачу событий zVirt в Kaspersky SIEM Cloud по syslog для одного кластера виртуализации:

1. В веб-интерфейсе zVirt в разделе **Ресурсы (Compute)** выберите **Кластеры (Clusters)**.
2. При изменении настроек существующего кластера:

   a. Нажмите **Имя (Name)** кластера, который хотите настроить (откроется его расширенное описание) или выделите нужный кластер левой кнопкой мыши.

   b. Нажмите **Изменить (Edit)**.

   c. В появившемся окне Изменить кластер (Edit Cluster) выберите закладку **Журналирование (Logging)**.
3. При создании нового кластера:

   a. Нажмите **Новый (New)**.

   b. В появившемся окне **Новый кластер (New Cluster)** выберите закладку **Журналирование (Logging)**.
4. Установите флажок **Определить адрес Syslog-сервера (Determine Syslog server address)**.
5. В поле ввода укажите данные коллектора в следующем формате: <IP-адрес или FQDN коллектора Kaspersky SIEM Cloud>:<порт коллектора Kaspersky SIEM Cloud>. Например: 192.168.1.5:1514.
6. Если вы хотите использовать протокол **TCP** вместо **UDP** для передачи событий, установите флажок **Использовать TCP-соединение (Use TCP connection)**.

Чтобы настроить передачу событий zVirt в Kaspersky SIEM Cloud по syslog для одного хоста виртуализации:

1. В веб-интерфейсе zVirt в разделе **Ресурсы (Compute)** выберите **Хосты (Hosts)**.
2. При изменении настроек существующего хоста:
   a. Нажмите **Имя (Name)** хоста, который хотите настроить (откроется его расширенное описание) или выделите нужный хост левой кнопкой мыши.
   b. Нажмите **Изменить (Edit)**.
   c. В появившемся окне **Изменить хост (Edit Host)** выберите закладку **Журналирование (Logging)**.
3. При создании нового хоста:
   a. Нажмите **Новый (New)**.
   b. В появившемся окне **Новый хост (New Host)** выберите закладку **Журналирование (Logging)**.
4. Установите флажок **Определить адрес Syslog-сервера (Determine Syslog server address)**.
5. В поле ввода укажите данные коллектора в следующем формате: <IP-адрес или FQDN коллектора Kaspersky SIEM Cloud>:<порт коллектора Kaspersky SIEM Cloud>. Например: 192.168.1.5:1514.
6. Если вы хотите использовать протокол **TCP** вместо **UDP** для передачи событий, установите флажок **Использовать TCP-соединение (Use TCP connection)**.

Система zVirt может передавать события журналов Engine во внешние системы в режиме установки Hosted Engine.

Чтобы настроить передачу событий журналов Engine из zVirt в Kaspersky SIEM Cloud выполните следующие действия:

1. В веб-интерфейсе zVirt в разделе **Ресурсы (Compute)** выберите **Виртуальные машины (Virtual Machines)**.
2. Выделите машину, на которой запущена виртуальная машина **HostedEngine**, и нажмите **Изменить (Edit)**.
3. В окне **Изменить виртуальную машину (Edit virtual machine)** перейдите в раздел **Журналирование (Logging)**.
4. Установите флажок **Определить адрес Syslog-сервера (Determine Syslog server address)**.
5. В поле ввода укажите данные коллектора в следующем формате: <IP-адрес или FQDN коллектора Kaspersky SIEM Cloud>:<порт коллектора Kaspersky SIEM Cloud>. Например: 192.168.1.5:1514.
6. Если вы хотите использовать протокол **TCP** вместо **UDP** для передачи журналов, установите флажок **Использовать TCP-соединение (Use TCP connection)**.

Настройка передачи событий системы zVirt в коллектор Kaspersky SIEM Cloud выполнена.

VipNet TIAS

Вы можете настроить получение событий VipNet TIAS в Kaspersky SIEM Cloud по протоколу syslog.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий VipNet TIAS в Kaspersky SIEM Cloud

1. Подключитесь к веб-интерфейсу VipNet TIAS под учетной записью с правами администратора.
2. Перейдите в раздел **Управление** – **Интеграции**.
3. На странице **Интеграция** перейдите на вкладку **Syslog**.
4. На панели инструментов списка принимающих серверов нажмите **Новый сервер**.
5. В открывшейся карточке нового сервера выполните следующие действия:
   a. В поле **Адрес сервера** укажите IP-адрес или доменное имя коллектора Kaspersky SIEM Cloud, например `10.1.2.3` или `syslog.siem.ru`.
   b. В поле **Порт** укажите входящий порт коллектора Kaspersky SIEM Cloud. По умолчанию указан порт 514.
   c. В списке **Протокол** выберите протокол транспортного уровня, который прослушивает коллектор Kaspersky SIEM Cloud. По умолчанию выбран протокол UDP.
   d. В списке **Организация** с помощью флажков выберите организации инфраструктуры ViPNet TIAS.
      Сообщения будут отправляться только по инцидентам, обнаруженным на основании событий, полученных от сенсоров выбранных организаций инфраструктуры.
   e. В списке **Статус** с помощью флажков выберите статусы инцидентов.
      Сообщения будут отправляться только при назначении инцидентам выбранных статусов.
   f. В списке **Уровень важности** с помощью флажков выберите уровни важности инцидентов.
      Сообщения будут отправляться только об инцидентах выбранных уровней важности. По умолчанию в списке выбран только высокий уровень важности.
   g. В списке **Язык интерфейса** выберите язык, на котором вы хотите получать информацию об инцидентах в сообщениях. По умолчанию выбран русский язык.
6. Нажмите кнопку **Добавить**.
7. В панели инструментов списка включите переключатель **Не передавать информацию об инцидентах в формате CEF**.
   При обнаружении новых и изменении статусов ранее выявленных инцидентов, в зависимости от выбранных при настройке статусов, будет выполняться передача соответствующей информации на указанные адреса принимающих серверов по протоколу syslog в формате CEF.
8. Нажмите **Сохранить изменения**.

Отправка событий в коллектор Kaspersky SIEM Cloud будет настроена.

2. Создание коллектора Kaspersky SIEM Cloud для получения событий VipNet TIAS

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Парсинг событий** выберите нормализатор **[OOTB] Syslog-CEF**.

3 Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий VipNet TIAS требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

4 Проверка поступления событий VipNet TIAS в Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий VipNet TIAS выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Zeek IDS

Вы можете настроить получение событий программы Zeek IDS версии 1.8 в Kaspersky SIEM Cloud.

Настройка получения событий состоит из следующих этапов:

1 Преобразование формата журнала событий Zeek IDS

По умолчанию события Zeek IDS записываются в файлы в директорию `/opt/zeek/logs/current`.

Нормализатор [OOTB] ZEEK IDS json file поддерживает работу с журналами Zeek IDS в формате JSON. Для передачи событий в нормализатор Kaspersky SIEM Cloud файлы журналов нужно преобразовать в формат JSON.

> Эту процедуру нужно повторять каждый раз перед получением событий Zeek IDS.

1. Подключитесь к серверу, на котором установлена программа Zeek IDS, под учетной записью с правами администратора.
2. Создайте директорию, где будут храниться журналы событий в формате JSON, с помощью команды:

   ```
   sudo mkdir /opt/zeek/logs/zeek-json
   ```

3. Перейдите в эту директорию с помощью команды:

   ```
   sudo cd /opt/zeek/logs/zeek-json
   ```

4. Выполните команду, которая с помощью утилиты jq преобразует исходный формат журнала событий к необходимому:

   ```
   jq . -c <path to the log file whose format needs to be changed> >> <new file name>.log
   ```

   Пример:

   ```
   jq . -c /opt/zeek/logs/current/conn.log >> conn.log
   ```

В директории `/opt/zeek/logs/zeek-json` будет создан новый файл, если такого ранее не существовало. Если такой файл уже был в текущей директории, то в конец файла будет добавлена новая информация.

❷ Создание коллектора Kaspersky SIEM Cloud для получения событий Zeek IDS

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Парсинг событий** выберите нормализатор **[OOTB] ZEEK IDS json file**, на шаге **Транспорт** выберите тип коннектора **file**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Zeek IDS требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Проверка поступления событий Zeek IDS в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий Zeek IDS выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Angie

Kaspersky SIEM Cloud позволяет осуществлять мониторинг событий аудита веб-сервера Angie или Angie Pro (версии 1.10.1 и выше), развернутого на устройствах под управлением операционных систем семейства Linux.

Настройка передачи и получения событий состоит из следующих этапов:

❶ Настройка передачи событий Angie

1. Проверьте синтаксис в конфигурационном файле на наличие ошибок, выполнив команду:

   ```
   sudo angie -t
   ```

   Возможные сообщения при проверке конфигурационного файла

   Если в конфигурационном файле синтаксические ошибки отсутствуют, Angie отобразит уведомления:

   ```
   angie: the configuration file /etc/angie/angie.conf syntax is ok
   angie: configuration file /etc/angie/angie.conf test is successful
   ```

   Если в конфигурационном файле найдены синтаксические ошибки, Angie сообщит, в чем заключается ошибка, например:

   ```
   angie: [emerg] "http" directive is not allowed here in etc/angie/http.d/angie-to-siem.conf:1
   angie: configuration file /etc/angie/angie.conf test failed
   ```

   Подробнее о синтаксисе конфигурационного файла см. в официальной документации Angie.

2. Если проверка синтаксиса прошла успешно (получен результат `test is successful`), выполните резервное копирование исходного конфигурационного файла с помощью следующей команды:

   ```
   sudo cp /etc/angie/angie.conf /etc/angie/angie_backup.conf
   ```

3. Откройте конфигурационный файл `angie.conf`, выполнив следующую команду:

```
sudo vi /etc/angie/angie.conf
```

Стандартный конфигурационный файл `angie.conf` по умолчанию располагается в директории `/etc/angie`.

Если в работе веб-сервера Angie используется нестандартный конфигурационный файл, необходимо открыть именно его. Вы можете узнать текущее расположение этого файла с помощью следующей команды:

```
sudo angie -V
```

Расположение файла указано в параметре `--config-path`.

4. Проверьте, что в контексте `http` указана директива `include`, которая разрешает управление конфигурацией с помощью дочерних конфигурационных файлов, выполнив следующую команду:

```
include /etc/angie/http.d/*.conf
```

5. Создайте конфигурационный файл `angie-to-siem.conf` в директории `/etc/angie/http.d/` с помощью следующей команды:

```
touch /etc/angie/http.d/angie-to-siem.conf
```

6. Откройте конфигурационный файл `angie-to-siem.conf`, выполнив команду:

```
sudo vi /etc/angie/http.d/angie-to-siem.conf
```

7. В директиве `log_format` укажите формат отправляемых событий следующим образом:

```
log_format syslog
device_event_category=access_log|time=$time_iso8601|version=$angie_version|http_method=$request_method|req_body=$r
```

8. В директиве `access_log` укажите способ отправки информации о событиях по протоколу Syslog следующим образом:

```
access_log syslog:server=<collector_IP>:<port> syslog
```

9. Если также необходимо отправлять информацию о событиях с ошибками, добавьте строку с директивой `error_log`:

```
error_log syslog:server=<collector_IP>:<port>
```

Формат сообщения из директивы `error_log` невозможно изменить и сообщение всегда передается в следующем виде:

```
YYYY/MM/DD HH:MM:SS [LEVEL] PID#TID: *CID MESSAGE
```

Где:

- `YYYY/MM/DD` – дата в формате год/месяц/день;
- `HH:MM:SS` – время в формате часы:минуты:секунды;
- `[LEVEL]` – уровень критичности ошибки;
- `PID#TID` – идентификаторы процесса (англ. PID) и потока (англ. TID);
- `*CID` – уникальный номер соединения (англ. Connection ID);
- `MESSAGE` – текст сообщения об ошибке или предупреждении.

10. Проверьте синтаксис в конфигурационном файле на наличие ошибок, выполнив команду (см. пункт 1 инструкции):

```
sudo angie -t
```

11. Перезагрузите конфигурацию, выполнив следующую команду:

```
sudo service angie reload
```

Передача событий из Angie будет настроена.

❷ Создание коллектора Kaspersky SIEM Cloud для событий Angie

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Парсинг событий** выберите нормализатор **[OOTB] Angie syslog**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Angie требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Проверка поступления событий Angie в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка поступления событий из Angie и Angie Pro выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Dallas Lock 8

Kaspersky SIEM Cloud позволяет осуществлять мониторинг событий системы Dallas Lock 8 версии 11.4.2, поступающих в формате CEF.

Настройка получения событий состоит из следующих этапов:

❶ Настройка отправки событий Dallas Lock 8

1. В Dallas Lock 8 перейдите в меню **Выгрузка журналов**.
2. Установите флажок **Экспорт журналов в SIEM-систему** и выполните следующие действия:
   a. В поле **Сервер** укажите IP-адрес или FQDN коллектора Kaspersky SIEM Cloud.
   b. В поле **Порт** укажите порт, который прослушивает коллектор Kaspersky SIEM Cloud.
   c. Выберите формат выгрузки **CEF**.
   d. Выберите кодировку выгрузки **UTF-8**.
3. Установите флажки рядом с типами событий, которые необходимо отправлять в Kaspersky SIEM Cloud.
4. В раскрывающемся списке **Период выгрузки журналов** выберите значение **1 минута**.
5. Нажмите на кнопку **OK**.

Отправка событий настроена.

❷ Создание коллектора Kaspersky SIEM Cloud для событий Dallas Lock 8

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Парсинг событий** выберите нормализатор **[OOTB] Confident Dallas Lock syslog CEF**. Также на вкладке **Транспорт** укажите те же порт и протокол, которые вы указали при настройке отправки событий.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Dallas Lock 8 требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Проверка поступления событий Dallas Lock 8 в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что сервер источника событий Dallas Lock 8 настроен правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Единый центр управления Dallas Lock

Kaspersky SIEM Cloud позволяет осуществлять мониторинг событий системы Единый центр управления Dallas Lock (далее ЕЦУ Dallas Lock) версии 4.0, поступающих в формате CEF.

Настройка получения событий состоит из следующих этапов:

1 Настройка отправки событий ЕЦУ Dallas Lock

1. В ЕЦУ Dallas Lock перейдите в меню **Экспорт инцидентов безопасности**.
2. Установите флажок **Экспорт инцидентов безопасности в SIEM-систему** и выполните следующие действия:
   a. В раскрывающемся списке **Формат** выберите формат **CEF**.
   b. В поле **Сервер** укажите IP-адрес или FQDN коллектора Kaspersky SIEM Cloud.
   c. В поле **Протокол** укажите протокол, который будет использоваться для передачи данных.
   d. В поле **Порт** укажите порт, который прослушивает коллектор Kaspersky SIEM Cloud.
3. Нажмите на кнопку **Применить**.

Отправка событий будет настроена.

2 Создание коллектора Kaspersky SIEM Cloud для событий ЕЦУ Dallas Lock

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Парсинг событий** выберите нормализатор **[OOTB] Confident Dallas Lock syslog CEF**. Также на вкладке **Транспорт** укажите те же порт и протокол, которые вы указали при настройке отправки событий.

3 Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения настройки коллектора для сбора событий ЕЦУ Dallas Lock требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

4 Проверка поступления событий ЕЦУ Dallas Lock в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что сервер источника событий ЕЦУ Dallas Lock настроен правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Базы данных и системы аудита СУБД

В этом разделе описана настройка получения событий СУБД и плагинов аудита баз данных.

PostgreSQL

Kaspersky SIEM Cloud позволяет осуществлять мониторинг и проводить аудит событий PostgreSQL на устройствах Linux с помощью rsyslog.

Аудит событий проводится с помощью плагина pgAudit. Плагин поддерживает работу с PostgreSQL версии 9.5 и выше. Подробную информацию о плагине pgAudit см. по ссылке: https://github.com/pgaudit/pgaudit.

Настройка получения событий состоит из следующих этапов:

1 Установка плагина pdAudit

1. В командном интерпретаторе выполните команды под учетной записью с правами администратора:

   ```
   sudo apt update
   sudo apt -y install postgresql-<версия базы данных PostgreSQL>-pgaudit
   ```

   Версию плагина необходимо выбрать в зависимости от версии PostgresSQL. Информацию о версиях PostgreSQL и необходимых версиях плагина см.по ссылке: https://github.com/pgaudit/pgaudit#postgresql-version-compatibility.

   Например

   ```
   sudo apt -y install postgresql-12-pgaudit
   ```

2. Найдите конфигурационный файл `postgres.conf`. Для этого в командной строке PostgresSQL выполните команду:

   ```
   show data_directory;
   ```

   В ответе будет указано расположение конфигурационного файла.

3. Создайте резервную копию конфигурационного файла `postgres.conf`.

4. Откройте файл `postgres.conf` и скопируйте или замените имеющиеся значения на указанные ниже.

```
```
pgAudit settings
shared_preload_libraries = 'pgaudit'
database logging settings
log_destination = 'syslog'
syslog facility
syslog_facility = 'LOCAL0'
event ident
syslog_ident = 'Postgres'
sequence numbers in syslog
syslog_sequence_numbers = on
split messages in syslog
syslog_split_messages = off
message encoding
lc_messages = 'en_US.UTF-8'
min message level for logging
client_min_messages = log
min error message level for logging
log_min_error_statement = info
log checkpoints (buffers, restarts)
log_checkpoints = off
log query duration
log_duration = off
error description level
log_error_verbosity = default
user connections logging
log_connections = on
user disconnections logging
log_disconnections = on
log prefix format
log_line_prefix = '%m|%a|%d|%p|%r|%i|%u| %e '
log_statement
log_statement = 'none'
hostname logging status. dns bane resolving affect
#performance!
log_hostname = off
logging collector buffer status
#logging_collector = off
pg audit settings
pgaudit.log_parameter = on
pgaudit.log='ROLE, DDL, MISC, FUNCTION'
```
```

5. Перезапустите службу PostgreSQL с помощью команды:

```
sudo systemctl restart postgresql
```

6. Загрузите плагин pgAudit в PostgreSQL. Для этого в командной строке PostgreSQL выполните команду:

```
CREATE EXTENSION pgaudit;
```

Плагин pgAudit будет установлен.

❷ Создание коллектора Kaspersky SIEM Cloud для получения событий PostgreSQL

Для получения событий PostgreSQL с помощью rsyslog при создании коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] PostgreSQL pgAudit syslog**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий PostgreSQL требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Настройка Syslog-сервера для отправки событий

Для передачи событий от сервера в Kaspersky SIEM Cloud используется сервис rsyslog.

1. Чтобы проверить, что на сервере источника событий установлен сервис rsyslog, выполните следующую команду под учетной записью с правами администратора:

   ```
   sudo systemctl status rsyslog.service
   ```

   Если сервис rsyslog не установлен на сервере, установите его, выполнив следующие команды:

   ```
   yum install rsyslog
   sudo systemctl enable rsyslog.service
   sudo systemctl start rsyslog.service
   ```

2. В директории `/etc/rsyslog.d/` создайте файл `pgsql-to-siem.conf` со следующим содержанием:

   ```
   If $programname contains 'Postgres' then @<collector IP address>:<collector port>
   ```

   Например

   ```
   If $programname contains 'Postgres' then @192.168.1.5:1514
   ```

   Если вы хотите отправлять события по протоколу TCP, содержимое файла должно быть таким:

   ```
   If $programname contains 'Postgres' then @@<collector IP address>:<collector port>
   ```

3. Сохраните изменения в конфигурационном файле `pgsql-to-siem.conf`.

4. В конфигурационный файл `/etc/rsyslog.conf` добавьте следующие строки:

   ```
   $IncludeConfig /etc/pgsql-to-siem.conf
   $RepeatedMsgReduction off
   ```

5. Сохраните изменения в конфигурационном файле `/etc/rsyslog.conf`.

6. Перезапустите сервис rsyslog, выполнив следующую команду:

   ```
   sudo systemctl restart rsyslog.service
   ```

❺ Проверка поступления событий PostgreSQL в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий PostgreSQL выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

MariaDB Audit Plugin

Kaspersky SIEM Cloud позволяет проводить аудит событий с помощью плагина MariaDB Audit Plugin. Плагин поддерживает работу с MySQL 5.7 и MariaDB. Работа плагина аудита с MySQL 8 не поддерживается. Подробная информация о плагине доступна на официальном веб-сайте MariaDB.

> Мы рекомендуем использовать плагин MariaDB Audit Plugin версии 1.2 и выше.

Настройка получения событий состоит из следующих этапов:

1. Настройка плагина MariaDB Audit Plugin

Вы можете настроить передачу событий с помощью плагина MariaDB Audit Plugin, используя одну из следующих инструкций:

Для передачи событий MySQL

Плагин MariaDB Audit Plugin поддерживается для MySQL 5.7 версии до 5.7.30 и поставляется в комплекте с MariaDB.

Чтобы настроить передачу событий MySQL 5.7 с помощью плагина MariaDB Audit Plugin:

1. Скачайте дистрибутив MariaDB и распакуйте его.

   Дистрибутив MariaDB доступен на официальном веб-сайте MariaDB. Операционная система дистрибутива MariaDB должна совпадать с операционной системой, на которой функционирует MySQL 5.7.

2. Подключитесь к MySQL 5.7 под учетной записью с правами администратора, выполнив команду:

   ```
   mysql -u <имя пользователя> -p
   ```

3. Чтобы получить директорию, в которой расположены плагины MySQL 5.7, в командной строке MySQL 5.7 выполните команду:

   ```
   SHOW GLOBAL VARIABLES LIKE 'plugin_dir'
   ```

4. В директории, полученной на шаге 3, скопируйте плагин MariaDB Audit Plugin из директории `<директория, куда был разархивирован дистрибутив>/mariadb-server-<версия>/lib/plugins/server_audit.so`.

5. В командном интерпретаторе операционной системы выполните команду:

   ```
   chmod 755 <директория, куда был разархивирован дистрибутив>server_audit.so
   ```

   Например

   ```
   chmod 755 /usr/lib64/mysql/plugin/server_audit.so
   ```

6. В командном интерпретаторе MySQL 5.7 выполните команду:

   `install plugin server_audit soname 'server_audit.so'`

7. Создайте резервную копию конфигурационного файла `/etc/mysql/mysql.conf.d/mysqld.cnf`.

8. В конфигурационном файле `/etc/mysql/mysql.conf.d/mysqld.cnf` в секции `[mysqld]` добавьте следующие строки:

   ```
   server_audit_logging=1
   server_audit_events=connect,table,query_ddl,query_dml,query_dcl
   server_audit_output_type=SYSLOG
   server_audit_syslog_facility=LOG_SYSLOG
   ```

   Если вы хотите отключить передачу событий для определенных групп событий аудита, удалите часть значений параметра `server_audit_events`. Описание параметров доступно на веб-сайте производителя плагина MariaDB Audit Plugin.

9. Сохраните изменения в конфигурационном файле.

10. Перезапустите сервис MariaDB, выполнив одну из следующих команд:

    - `systemctl restart mysqld` – для системы инициализации systemd.
    - `service mysqld restart` – для системы инициализации init.

Настройка плагина MariaDB Audit Plugin для MySQL 5.7 завершена. При необходимости вы можете выполнить следующие команды в командной строке MySQL 5.7:

- `show plugins` – для проверки списка текущих плагинов.
- `SHOW GLOBAL VARIABLES LIKE 'server_audit%'` – для проверки текущих настроек аудита.

Для передачи событий MariaDB

Плагин MariaDB Audit Plugin входит в состав дистрибутива MariaDB, начиная с версий 5.5.37 и 10.0.10.

Чтобы настроить передачу событий MariaDB с помощью плагина MariaDB Audit Plugin:

1. Подключитесь к MariaDB под учетной записью с правами администратора, выполнив команду:

   ```
   mysql -u <имя пользователя> -p
   ```

2. Чтобы проверить, что плагин есть в директории, где размещены плагины операционной системы, в командной строке MariaDB выполните команду:

   ```
   SHOW GLOBAL VARIABLES LIKE 'plugin_dir'
   ```

3. В командном интерпретаторе операционной системы выполните команду:

   ```
   ll <директория, полученная в результате выполнения предыдущей команды> | grep server_audit.so
   ```

   Если вывод команды пуст и плагина нет в директории, вы можете скопировать плагин MariaDB Audit Plugin в эту директорию или использовать более новую версию MariaDB.

4. В командном интерпретаторе MariaDB выполните команду:

```
install plugin server_audit soname 'server_audit.so'
```

5. Создайте резервную копию конфигурационного файла `/etc/mysql/my.cnf`.

6. В конфигурационном файле `/etc/mysql/my.cnf` в разделе `[mysqld]` добавьте следующие строки:

```
server_audit_logging=1
server_audit_events=connect,table,query_ddl,query_dml,query_dcl
server_audit_output_type=SYSLOG
server_audit_syslog_facility=LOG_SYSLOG
```

   Если вы хотите отключить передачу событий для определенных групп событий аудита, удалите часть значений параметра `server_audit_events`. Описание параметров доступно на веб-сайте производителя плагина MariaDB Audit Plugin.

7. Сохраните изменения в конфигурационном файле.

8. Перезапустите сервис MariaDB, выполнив одну из следующих команд:

   - `systemctl restart mariadb` – для системы инициализации systemd.
   - `service mariadb restart` – для системы инициализации init.

Настройка плагина MariaDB Audit Plugin для MariaDB завершена. При необходимости вы можете выполнить следующие команды в командной строке MariaDB:

- `show plugins` – для проверки списка текущих плагинов.
- `SHOW GLOBAL VARIABLES LIKE 'server_audit%'` – для проверки текущих настроек аудита.

❷ Создание коллектора Kaspersky SIEM Cloud для событий MySQL 5.7 или MariaDB

Для получения событий MySQL 5.7 и MariaDB с помощью плагина MariaDB Audit Plugin при создании коллектора Kaspersky SIEM Cloud на шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] MariaDB Audit Plugin syslog**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий MySQL 5.7 или MariaDB требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

4 Настройка Syslog-сервера для отправки событий

Для передачи событий от сервера в коллектор используется сервис rsyslog.

1. Перед внесением изменений создайте резервную копию конфигурационного файла `/etc/rsyslog.conf`.
2. Для отправки событий по протоколу UDP добавьте в конфигурационный файл `/etc/rsyslog.conf` строку:

   ```
   *.* @<Kaspersky SIEM Cloud collector IP address>:<Kaspersky SIEM Cloud collector port>
   ```

   Например

   ```
   *.* @192.168.1.5:1514
   ```

   Если вы хотите отправлять события по протоколу TCP, строка должна выглядеть следующим образом:

   ```
   *.* @@192.168.1.5:2514
   ```

3. Сохраните изменения в конфигурационном файле `/etc/rsyslog.conf.`
4. Перезапустите сервис rsyslog, выполнив следующую команду:

   ```
   sudo systemctl restart rsyslog.service
   ```

5 Проверка поступления событий MySQL и MariaDB в коллектор Kaspersky SIEM Cloud

Чтобы проверить, что настройка сервера источника событий MySQL и MariaDB выполнена правильно, вы можете осуществить поиск связанных событий.

Apache Cassandra

Kaspersky SIEM Cloud позволяет получать информацию о событиях Apache Cassandra.

Настройка получения событий состоит из следующих этапов:

1 Настройка журналирования событий Apache Cassandra в Kaspersky SIEM Cloud

1. Убедитесь, что на сервере, где установлена Apache Cassandra, есть 5 ГБ свободного дискового пространства.
2. Подключитесь к серверу Apache Cassandra под учетной записью с правами администратора.
3. Перед внесением изменений создайте резервные копии следующих конфигурационных файлов `/etc/cassandra/cassandra.yaml` и `/etc/cassandra/logback.xml`.

4. Убедитесь, что параметры конфигурационного файла `/etc/cassandra/cassandra.yaml` имеют следующие значения, и при необходимости внесите изменения:

   a. В секции `audit_logging_options` присвойте параметру `enabled` значение `true.`

   b. В секции `logger` присвойте параметру `class_name` значение `FileAuditLogger`.

5. В конфигурационный файл `/etc/cassandra/logback.xml` добавьте следующие строки:

```
<!-- Audit Logging (FileAuditLogger) rolling file appender to audit.log -->
<appender name="AUDIT" class="ch.qos.logback.core.rolling.RollingFileAppender">
  <file>${cassandra.logdir}/audit/audit.log</file>
 <rollingPolicy class="ch.qos.logback.core.rolling.SizeAndTimeBasedRollingPolicy">
    <!-- rollover daily -->
    <fileNamePattern>${cassandra.logdir}/audit/audit.log.%d{yyyy-MM-dd}.%i.zip</fileNamePattern>
    <!-- each file should be at most 50MB, keep 30 days worth of history, but at most 5GB -->
    <maxFileSize>50MB</maxFileSize>
    <maxHistory>30</maxHistory>
    <totalSizeCap>5GB</totalSizeCap>
  </rollingPolicy>
  <encoder>
    <pattern>%-5level [%thread] %date{ISO8601} %F:%L - %replace(%msg){'\n', ' '}%n</pattern>
  </encoder>
</appender>

<!-- Audit Logging additivity to redirect audt logging events to audit/audit.log -->
<logger name="org.apache.cassandra.audit" additivity="false" level="INFO">
    <appender-ref ref="AUDIT"/>
</logger>
```

6. Сохраните изменения в конфигурационном файле.

7. Перезапустите службу Apache Cassandra с помощью следующих команд:

```
sudo systemctl stop cassandra.service
```

```
sudo systemctl start cassandra.service
```

8. После перезапуска проверьте статус Apache Cassandra с помощью следующей команды:

```
sudo systemctl status cassandra.service
```

   Убедитесь, что в выводе команды есть последовательность символов:

```
Active: active (running)
```

Настройка передачи событий Apache Cassandra завершена. События будут располагаться в директории `/var/log/cassandra/audit/`, в файле `audit.log` (`${cassandra.logdir}/audit/audit.log`).

❷ Создание коллектора Kaspersky SIEM Cloud для событий Apache Cassandra

Для получения событий Apache Cassandra при создании коллектора Kaspersky SIEM Cloud необходимо выполнить следующие действия: на шаге **Транспорт** выберите коннектор типа **file**, на шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] Apache Cassandra file**.

3 Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Apache Cassandra требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

4 Проверка поступления событий Apache Cassandra в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий Apache Cassandra выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Облачные и виртуальные платформы

В этом разделе описана настройка получения событий облачных платформ, виртуальных машин и систем резервного копирования.

Nextcloud

Вы можете настроить получение событий программы Nextcloud 26.0.4 в Kaspersky SIEM Cloud.

Настройка получения событий состоит из следующих этапов:

1 Настройка аудита событий Nextcloud

1. На сервере, на котором установлена программа Nextcloud, создайте резервную копию конфигурационного файла `/home/localuser/www/nextcloud/config/config.php`.
2. Измените конфигурационный файл Nextcloud `/home/localuser/www/nextcloud/config/config.php`.
3. Измените значения следующих параметров на приведенные ниже:

```
'log_type' => 'syslog',
'syslog_tag' => 'Nextcloud',
'logfile' => '',
'loglevel' => 0,
'log.condition' => [
    'apps' => ['admin_audit'],
],
```

4. Перезагрузите сервис Nextcloud с помощью команды:

```
sudo service restart nextcloud
```

Настройка отправки событий в коллектор Kaspersky SIEM Cloud будет выполнена.

❷ Настройка Syslog-сервера для отправки событий

Для передачи событий от сервера в коллектор используется сервис rsyslog.

1. В директории `/etc/rsyslog.d/` создайте файл `Nextcloud-to-siem.conf` со следующим содержанием:

   ```
   If $programname contains 'Nextcloud' then @<collector IP address>:<collector port>
   ```

   Пример:

   ```
   If $programname contains 'Nextcloud' then @192.168.1.5:1514
   ```

   Если вы хотите отправлять события по протоколу TCP, содержимое файла должно быть таким:

   ```
   If $programname contains 'Nextcloud' then @@<collector IP address>:<collector port>
   ```

2. Сохраните изменения в конфигурационном файле `Nextcloud-to-siem.conf`.

3. Создайте резервную копию файла `/etc/rsyslog.conf`.

4. В конфигурационный файл `/etc/rsyslog.conf` добавьте следующие строки:

   ```
   $IncludeConfig /etc/Nextcloud-to-siem.conf
   $RepeatedMsgReduction off
   ```

5. Сохраните внесенные изменения.

6. Перезапустите сервис rsyslog, выполнив следующую команду:

   ```
   sudo systemctl restart rsyslog.service
   ```

Передача событий Nextcloud в коллектор будет настроена.

❸ Создание коллектора Kaspersky SIEM Cloud для получения событий Nextcloud

Для получения событий Nextcloud при создании коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] Nextcloud syslog**, на шаге **Транспорт** выберите тип коннектора **tcp** или **udp**.

❹ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Nextcloud требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❺ Проверка поступления событий Nextcloud в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий Nextcloud выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Yandex Cloud

Настройка получения событий от системы Yandex Cloud в Kaspersky SIEM Cloud состоит из следующих этапов.

1. Настройка аудита событий Yandex Cloud

Настройка передачи событий включает следующие шаги:

1. Подготовка среды для работы с Yandex Cloud

Для выполнения работ по настройке необходим Yandex Cloud CLI, установите и инициализируйте его.

Примечание: по умолчанию аудит будет осуществляться в каталоге Yandex Cloud, указанном в профиле CLI. Вы можете указать другой каталог с помощью параметра `--folder-name` или `--folder-id`.

Для настройки аудита необходим активный платежный аккаунт, поскольку за использование инфраструктуры Yandex Cloud взимается плата.

Чтобы настроить аудит Yandex Cloud, требуется активный платежный аккаунт:

1. Перейдите в консоль управления, затем войдите в Yandex Cloud или зарегистрируйтесь.
2. На странице Yandex Cloud Billing убедитесь, что у вас подключен платежный аккаунт, и он находится в статусе ACTIVE или TRIAL_ACTIVE. Если платежного аккаунта нет, создайте его.

Если у вас есть активный платежный аккаунт, вы можете создать или выбрать каталог Yandex Cloud, в котором будет работать ваша инфраструктура, на странице облака.

2. Создание бакета для аудитных логов

Чтобы создать бакет:

1. В консоли управления перейдите в каталог, в котором хотите создать бакет, например, **example-folder**.
2. Выберите сервис **Object Storage**.
3. Нажмите **Создать бакет**.
4. На странице создания бакета выполните следующие действия:
   a. Введите имя бакета в соответствии с правилами именования, например, **kumabucket**.
   b. При необходимости ограничьте максимальный размер бакета. Размер 0 означает отсутствие ограничений и аналогичен включенной опции **Без ограничения**.
   c. Выберите тип доступа **Ограниченный**.
   d. Выберите класс хранилища по умолчанию.
   e. Нажмите **Создать бакет**.

Бакет создан.

3. Создание ключа шифрования в сервисе Key Management Service

Чтобы создать ключ шифрования:

1. В консоли управления перейдите в каталог **example-folder**.
2. Выберите сервис **Key Management Service**.
3. Нажмите **Создать ключ** и укажите следующие параметры:
   - Имя – например, **kuma-kms**.
   - Алгоритм шифрования – **AES-256**.
   - Для остальных параметров оставьте значения по умолчанию.
4. Нажмите **Создать**.

Ключ шифрования создан.

4. Включение шифрования бакета

Чтобы включить шифрование бакета:

1. В консоли управления перейдите в бакет, созданный ранее.
2. На панели слева выберите **Шифрование**.
3. В поле **Ключ KMS** выберите ключ **kuma-kms**.
4. Нажмите **Сохранить**.

Шифрование бакета включено.

5. Создание сервисных аккаунтов

Чтобы создать сервисные аккаунты – отдельный аккаунт для трейла и отдельный аккаунт бакета, выполните следующие шаги:

1. Создайте сервисный аккаунт **sa-kuma**:
   1. В консоли управления перейдите в каталог **example-folder**.
   2. В верхней части экрана перейдите на вкладку **Сервисные аккаунты**.
   3. Нажмите **Создать сервисный аккаунт** и введите имя сервисного аккаунта, например **sa-kuma**, в соответствии с правилами именования:
      - длина – от 3 до 63 символов;
      - может содержать строчные буквы латинского алфавита, цифры и дефисы;
      - первый символ – буква, последний – не дефис.
   4. Нажмите **Создать**.

2. Создайте сервисный аккаунт **sa-kuma-bucket**:

    1. В консоли управления перейдите в каталог **example-folder**.

    2. В верхней части экрана перейдите на вкладку **Сервисные аккаунты**.

    3. Нажмите **Создать сервисный аккаунт** и введите имя сервисного аккаунта, например **sa-kuma-bucket**, в соответствии с правилами именования:

        - длина – от 3 до 63 символов;
        - может содержать строчные буквы латинского алфавита, цифры и дефисы;
        - первый символ – буква, последний – не дефис.

    4. Нажмите **Создать**.

    Сервисные аккаунты созданы.

6. Создание статического ключа

Идентификатор ключа и секретный ключ понадобятся на этапе монтирования бакета. Ключ можно создать с помощью консоли управления или с помощью CLI.

Чтобы создать ключ с помощью консоли управления:

1. В консоли управления перейдите в каталог **example-folder**.

2. В верхней части экрана перейдите на вкладку **Сервисные аккаунты**.

3. Выберите сервисный аккаунт **sa-kuma-bucket** и нажмите на строку с его именем.

4. На верхней панели нажмите **Создать новый ключ**.

5. Выберите **Создать статический ключ доступа**.

6. Задайте описание ключа и нажмите **Создать**.

7. Сохраните идентификатор и секретный ключ.

Статический ключ доступа создан. После закрытия диалога значение ключа будет недоступно.

Чтобы создать ключ с помощью CLI:

1. Создайте ключ доступа для сервисного аккаунта **sa-kuma-bucket**:

   ```
   yc iam access-key create --service-account-name sa-kuma-bucket
   ```

   Результат: `ls`

   ```
   access_key:
     id: aje*******k2u
     service_account_id: aje*******usm
     created_at: "2022-09-22T14:37:51Z"
     key_id: 0n8*******0YQ
   secret: JyT*******zMP1
   ```

2. Сохраните идентификатор key_id и секретный ключ secret. Получить значение ключа повторно будет невозможно.

Ключ доступа создан.

7. Назначение роли сервисным аккаунтам

Чтобы назначить сервисному аккаунту sa-kuma роли audit-trails.viewer, storage.uploader и kms.keys.encrypterDecrypter:

1. В CLI назначьте роль audit-trails.viewer на каталог:

   ```
   yc resource-manager folder add-access-binding \
   --role audit-trails.viewer \
   --id <directory_id> \
   --service-account-id <service_account_id>
   ```

   Где:

   - `--role` – назначаемая роль;
   - `--id` – идентификатор каталога example-folder;
   - `--service-account-id` – идентификатор сервисного аккаунта sa-kuma.

2. Назначьте роль storage.uploader на каталог с бакетом:

   ```
   yc resource-manager folder add-access-binding \
   --role storage.uploader \
   --id <directory_id> \
   --service-account-id <service_account_id>
   ```

   Где:

   - `--role` – назначаемая роль;
   - `--id` – идентификатор каталога example-folder;
   - `--service-account-id` – идентификатор сервисного аккаунта sa-kuma.

3. Назначьте роль kms.keys.encrypterDecrypter на ключ шифрования kuma-kms:

```
yc kms symmetric-key add-access-binding \
--role kms.keys.encrypterDecrypter \
--id <key_id> \
--service-account-id <service_account_id>
```

Где:

- `--role` – назначаемая роль;
- `--id` – идентификатор KMS-ключа kuma-kms;
- `--service-account-id` – идентификатор сервисного аккаунта sa-kuma.

Чтобы назначить сервисному аккаунту sa-kuma-bucket роли storage.viewer и kms.keys.encrypterDecrypter:

1. В CLI назначьте роль storage.viewer на каталог:

```
yc resource-manager folder add-access-binding \
--id <directory_id> \
--role storage.viewer \
--service-account-id <service_account_id>
```

Где:

- `--id` – идентификатор каталога example-folder;
- `--role` – назначаемая роль;
- `--service-account-id` – идентификатор сервисного аккаунта sa-kuma-bucket.

2. Назначьте роль kms.keys.encrypterDecrypter на ключ шифрования kuma-kms:

```
yc kms symmetric-key add-access-binding \
--role kms.keys.encrypterDecrypter \
--id <key_id> \
--service-account-id <service_account_id>
```

Где:

- `--role` – назначаемая роль;
- `--id` – идентификатор KMS-ключа kuma-kms;
- `--service-account-id` – идентификатор сервисного аккаунта sa-kuma-bucket.

8. Создание аудит трейла

Чтобы создать аудит трейл:

1. В консоли управления перейдите в каталог **example-folder**.
2. Выберите сервис **Audit Trails**.
3. Нажмите **Создать трейл** и укажите имя создаваемого трейла, например, **kuma-trail**.

4. В блоке **Назначение** задайте параметры объекта назначения:

   - **Назначение** – **Object Storage**.
   - **Бакет** – имя бакета, например, **kumabucket**.
   - **Префикс объекта** – необязательный параметр, участвует в полном имени файла аудитного лога.

     Используйте префикс, если вы храните аудитные логи и сторонние данные в одном и том же бакете. Не используйте одинаковый префикс для логов и других объектов в бакете, так как в этом случае логи и сторонние объекты могут перезаписать друг друга.
   - **Ключ шифрования** – укажите ключ шифрования kuma-kms, которым зашифрован бакет.

5. В блоке **Сервисный аккаунт** выберите **sa-kuma**.

6. В блоке **Сбор событий с уровня конфигурации** задайте параметры сбора аудитных логов уровня конфигурации:

   - **Сбор событий** – выберите **Включено**.
   - **Ресурс** – выберите **Каталог**.
   - **Каталог** – не требует заполнения, содержит имя текущего каталога.

7. В блоке **Сбор событий с уровня сервисов** в поле **Сбор событий** выберите **Выключено**.

8. Нажмите **Создать**.

❷ Настройка передачи событий Yandex Cloud

Бакет необходимо смонтировать на сервере, на котором будет установлен коллектор Kaspersky SIEM Cloud.

1. На сервере создайте директорию для пользователя kuma:

   ```
   sudo mkdir /home/kuma
   ```

2. На сервере создайте файл со статическим ключом доступа сервисного аккаунта sa-kuma-bucket и предоставьте на него права пользователю kuma:

   ```
   sudo bash -c 'echo <access_key_id>:<secret_access_key> > /home/kuma/.passwd-s3fs'
   sudo chmod 600 /home/kuma/.passwd-s3fs
   sudo chown -R kuma:kuma /home/kuma
   ```

3. Установите пакет s3fs:

   ```
   sudo apt install s3fs
   ```

4. Создайте директорию, в которую будет монтироваться бакет, и предоставьте на него права пользователю kuma:

   ```
   sudo mkdir /var/log/yandex-cloud/
   sudo chown kuma:kuma /var/log/yandex-cloud/
   ```

5. Смонтируйте бакет:

```
sudo s3fs kumabucket /var/log/yandex-cloud -o passwd_file=/home/kuma/.passwd-s3fs -o
url=https://storage.yandexcloud.net -o use_path_request_style -o uid=$(id -u kuma) -o gid=$(id -g kuma)
```

Вы можете настроить монтирование бакета при запуске операционной системы, для этого добавьте в файл /etc/fstab строку вида:

```
s3fs#kumabucket /var/log/yandex-cloud fuse _netdev,uid=<kuma_uid>,gid=
<kuma_gid>,use_path_request_style,url=https://storage.yandexcloud.net,passwd_file=/home/kuma/.passwd-s3fs 0 0
```

Где:

- `<kuma_uid>` – идентификатор пользователя kuma в операционной системе.
- `<kuma_gid>` – идентификатор группы пользователей kuma в операционной системе.

Чтобы узнать `kuma_uid` и `kuma_gid`, в консоли выполните команду:

```
id kuma
```

6. Проверьте, что бакет смонтирован:

```
sudo ls /var/log/yandex-cloud/
```

Если все настроено верно, команда вернет `<audit_trail_id>`, где `<audit_trail_id>` – идентификатор трейла аудита.

Настройка передачи событий Yandex Cloud завершена. События будут располагаться в директориях в файлах с расширением JSON:

```
/var/log/yandex-cloud/{audit_trail_id}/{year}/{month}/{day}/*.json
```

❸ Настройка коллектора Kaspersky SIEM Cloud для получения и обработки событий Yandex Cloud

Для получения событий Yandex Cloud при создании коллектора Kaspersky SIEM Cloud необходимо выполнить следующие действия:

1. В мастере установки коллектора Kaspersky SIEM Cloud на шаге **Транспорт** выберите коннектор типа **file**.
2. В поле **URL** укажите следующее:

```
/var/log/yandex-cloud/<audit_trail_id>/*/*/*/*.json
```

Где `<audit_trail_id>` – идентификатор аудита.

3. На шаге **Парсинг событий** в поле **Нормализатор** выберите **[OOTB] Yandex Cloud**.

4 Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Yandex Cloud требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

5 Проверка поступления событий Yandex Cloud в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий Yandex Cloud выполнена правильно, выполнив поиск связанных событий.

VMware vCenter

Вы можете настроить получение событий VMware vCenter в Kaspersky SIEM Cloud.

Настройка получения событий состоит из следующих этапов:

1 Настройка подключения к VMware vCenter

1. Подключитесь к веб-интерфейсу VMware Vcenter под учетной записью с правами администратора.
2. Перейдите в раздел **Security&Users** и выберите **Users**.
3. Создайте учетную запись пользователя.
4. Перейдите в раздел **Roles** и назначьте созданной учетной записи роль **Read-only: See details of objects, but not make changes**.

   Учетные данные этой записи вы будете использовать в секрете коллектора.

   Более подробная информация о создании учетных записей представлена в документации системы VMware Vcenter.

Настройка подключения к VMware vCenter для получения событий будет выполнена.

2 Создание коллектора Kaspersky SIEM Cloud для получения событий VMware vCenter

Для получения событий VMWare Vcenter при создании коллектора на шаге **Транспорт** выберите тип коннектора **vmware** и укажите обязательные параметры:

- URL, по которому доступен API VMware, например `https://vmware-server.com:6440`.
- Учетные данные VMware – секрет, в котором указаны логин и пароль для подключения к API VMware.

На шаге **Парсинг событий** выберите нормализатор **[OOTB] VMware vCenter API**.

3 Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий VMware vCenter требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

4 Проверка поступления событий VMWare Vcenter в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий VMWare Vcenter выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Veeam Backup & Replication

Kaspersky SIEM Cloud позволяет осуществлять мониторинг событий системы Veeam Backup & Replication (версия 12.1), поступающих по протоколу syslog.

Настройка получения событий Veeam Backup & Replication состоит из следующих этапов:

1 Настройка передачи событий Veeam Backup & Replication

Настройку передачи событий необходимо выполнять под учетной записью с правами администратора:

1. В веб-интерфейсе Veeam Backup & Replication откройте раздел **Параметры** → **Пересылка событий**.
2. В разделе **Серверы Syslog** нажмите **Добавить**.
3. В поле **Сервер** укажите полное доменное имя (FQDN) или IPv4-адрес сервера коллектора Kaspersky SIEM Cloud. Указать IPv6-адрес в этом поле невозможно.
4. В поле **Порт** укажите порт, который прослушивает коллектор Kaspersky SIEM Cloud.

   По умолчанию система Veeam Backup & Replication выполняет отправку событий на следующие порты в зависимости от используемого протокола:

   - 514 для TCP и UDP;
   - 6514 для TLS.
5. В раскрывающемся списке **Транспорт** выберите протокол: **TCP**, **UDP** или **TLS**.
6. Нажмите **OK**.

Передача событий из Veeam Backup & Replication в коллектор Kaspersky SIEM Cloud будет настроена.

2 Создание коллектора Kaspersky SIEM Cloud для получения событий Veeam Backup & Replication

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud на шаге **Транспорт** нужно указать тип коннектора, который используется при настройке передачи событий. Для получения событий Veeam Backup & Replication на шаге **Парсинг событий** нужно выбрать нормализатор **[OOTB] Veeam Software Veeam Backup & Replication syslog**.

3 Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Veeam Backup & Replication требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

4. Проверка поступления событий Veeam Backup & Replication в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что поступление событий из Veeam Backup & Replication настроено правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Почтовые и коллаборационные системы

В этом разделе описана настройка получения событий почтовых серверов и платформ совместной работы.

CommuniGate Pro

Вы можете настроить получение событий системы CommuniGate Pro версий 6.1 и 6.5.1 в Kaspersky SIEM Cloud. Интеграция возможна только при отправке событий по syslog с использованием протокола TCP. Поддерживается обработка части событий модуля SIP (события содержат последовательность символов "SIPDATA").

Система CommuniGate Pro формирует событие аудита в виде нескольких отдельных записей, которые выглядят следующим образом:

```
<код события> временная отметка идентификатор направление: информация из базового события 1

<код события> временная отметка идентификатор направление: информация из базового события 2

<код события> временная отметка идентификатор направление: основная информация n
```

Для обработки событий системы CommuniGate Pro используется набор ресурсов Kaspersky SIEM Cloud, который необходимо применить при создании коллектора:

- Нормализатор.
- Правило агрегации.
- Фильтры для точек назначения.

В процессе работы коллектора многострочные базовые события будут агрегированы на основе идентификатора событий, нормализованы, и одно событие будет направлено в хранилище и коррелятор.

Агрегированное событие примет следующий вид:

```
Служебная информация из правила агрегации: идентификатор: информация из базового события 1, информация из базового события 2, информация из базового события n
```

После агрегации полученное событие будет направлено в этот же коллектор, где будет выполняться нормализация агрегированного события.

Алгоритм обработки события системы CommuniGate Pro

Для обработки события системы CommuniGate Pro был реализован следующий алгоритм:

1. Первичная нормализация.

   На этом этапе выполняется первичная нормализация базовых событий. Первым символом в базовом событии является число. События приводятся к формату, пригодному для последующей агрегации: из события выделяется первый символ и размещается в поле DeviceCustomString1, идентификатор размещается в поле ExternalID, имя хоста размещается в поле DeviceHostName. Базовая нормализация выполняется в основном нормализаторе.

2. Проверка на агрегацию.

   Выполняется проверка, является ли событие агрегированным. В результате проверки к неагрегированным событиям (первый символ события является числом) применяется правило агрегации, а затем агрегированные события направляются на повторную нормализацию. Агрегация выполняется с помощью правила **[OOTB] CommuniGate Pro. Aggregation rule**.

3. Применение правила агрегации.

   На этом этапе к событиям применяется правило агрегации, базовые события "склеиваются" и принимают следующий вид:

   Служебная информация из правила агрегации: идентификатор: информация из базового события 1, информация из базового события 2, информация из базового события n.

   После выполнения агрегации "склеенное" событие направляется обратно в этот же коллектор для выполнения нормализации агрегированного события.

   Чтобы замкнуть цикл обработки события, следует указать тот же самый коллектор в качестве точки назначения. На схеме точка назначения названа "Loop", чтобы обозначить цикл обработки события. Вы можете назвать точку назначения произвольным именем.

4. Нормализация агрегированного события.

   Нормализация агрегированного события. начинающегося с символа "{", выполняется в экстранормализаторах Aggregated events, Aggregated events - kv part.

5. Отправка в хранилище и коррелятор.

   Агрегированные и нормализованные события отправляются в хранилище и коррелятор.

На следующем рисунке представлена схема обработки событий от системы CommuniGate Pro.

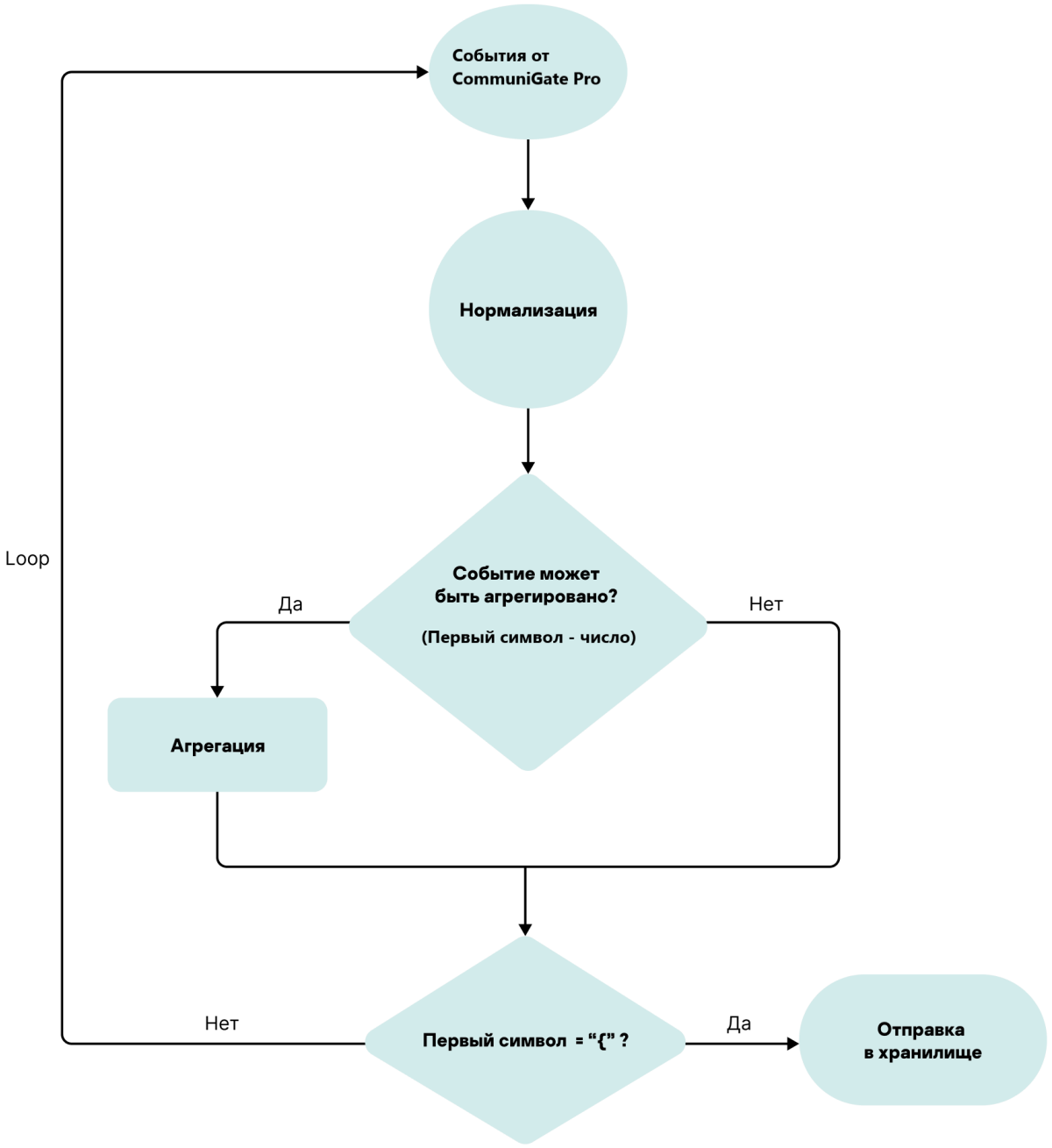


Схема обработки событий от системы CommuniGate Pro

Настройка получения событий состоит из следующих этапов:

1. Настройка CommuniGate Pro для отправки событий

События аудита системы CommuniGate Pro по умолчанию направляются в директорию `/var/CommuniGate/SystemLogs/` в файлы журналов с расширением LOG.

Для отправки событий в Kaspersky SIEM Cloud необходимо установить на сервер CommuniGate Pro агент Kaspersky SIEM Cloud и настроить чтение файлов с расширением LOG из директории `/var/CommuniGate/SystemLogs/` и отправку по протоколу TCP в коллектор Kaspersky SIEM Cloud.

1. В веб-интерфейсе откройте раздел **Мониторинг → Ресурсы и сервисы → Агенты** и нажмите **Добавить**.
2. В открывшемся окне **Создание агента** на вкладке **Основные параметры** в поле **Название** укажите название агента.
3. Перейдите на вкладку **Подключение №1**.
4. В блоке параметров **Коннектор** на вкладке **Основные параметры** задайте следующие значения для коннектора:
   a. В поле **Название** укажите название, например `CommuniGate file`.
   b. В раскрывающемся списке **Тип** выберите значение **file**.
   c. В поле **Путь к файлу** укажите значение:

   ```
   /var/CommuniGate/SystemLogs/.*.log
   ```

5. В блоке параметров **Точки назначения** на вкладке **Основные параметры** задайте следующие значения для точки назначения:
   a. В поле **Название** укажите название, например `CommuniGate TCP collector`.
   b. В раскрывающемся списке **Тип** выберите значение **tcp**.
   c. В поле **URL** укажите FQDN или IP-адрес и порт коллектора Kaspersky SIEM Cloud.
6. Нажмите на кнопку **Создать**.

После того как сервис агента будет создан, нужно установить агент на устройствах сетевой инфраструктуры, с которых вы хотите передавать данные в коллектор.

2 Создание коллектора Kaspersky SIEM Cloud для получения событий CommuniGate Pro

1. Импортируйте пакет [OOTB] CommuniGate Pro из репозитория Kaspersky SIEM Cloud.
2. Создайте новый коллектор и в мастере установки коллектора настройте следующие параметры:
   a. На шаге **Транспорт** в поле **Тип** выберите тип **tcp**, в поле **URL** укажите FQDN или IP-адрес и порт коллектора.
   b. На шаге **Парсинг событий** нажмите **Добавить парсинг событий** и в открывшемся окне **Основной парсинг событий** в раскрывающемся списке **Нормализатор** выберите нормализатор **[OOTB] CommuniGate Pro**.
   c. На шаге **Агрегация событий** нажмите **Добавить правило агрегации** и в открывшемся окне **Агрегация событий** в раскрывающемся списке **Правило агрегации** выберите правило агрегации **[OOTB] CommuniGate Pro. Aggregation rule**.

d. На шаге **Маршрутизация** нажмите **Добавить** и в открывшемся окне **Создание точки назначения** последовательно создайте три точки назначения: этот же коллектор с именем `Loop`, хранилище и коррелятор:

1. Создайте точку назначения с именем `Loop` со следующими параметрами:

   - На вкладке **Основные параметры** в раскрывающемся списке **Тип** выберите тип транспорта **tcp**, в поле **URL** укажите FQDN или IP-адрес и порт коллектора, указанные ранее на шаге 2.1 этой инструкции.
   - На вкладке **Дополнительные параметры** в раскрывающемся списке **Фильтр** выберите фильтр **[OOTB] CommuniGate Pro. Filter for event aggregation**.

   Настройка этих параметров необходима для отправки агрегированного события в тот же самый коллектор для дальнейшей нормализации.

2. Создайте точку назначения коррелятора:

   - На вкладке **Основные параметры** в раскрывающемся списке **Тип** выберите **correlator** и заполните поле **URL**.
   - На вкладке **Дополнительные параметры** в раскрывающемся списке **Фильтр** выберите фильтр **[OOTB] CommuniGate Pro. Aggregated events to storage and correlator**.

3. Создайте точку назначения хранилища:

   - На вкладке **Основные параметры** в раскрывающемся списке **Тип** выберите **storage** и заполните поле **URL**.
   - На вкладке **Дополнительные параметры** в раскрывающемся списке **Фильтр** выберите фильтр **[OOTB] CommuniGate Pro. Aggregated events to storage and correlator**.

   Настройка этих параметров необходима для отправки агрегированного нормализованного события в хранилище и коррелятор.

3. Нажмите на кнопку **Создать**.

   Сервис коллектора с заданными параметрами будет создан. На экране отобразится команда для установки сервиса на сервере.

4. Скопируйте команду для установки коллектора Kaspersky SIEM Cloud.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий CommuniGate Pro требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Проверка поступления событий CommuniGate Pro в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий CommuniGate Pro выполнена правильно, выполнив поиск связанных событий.

Postfix

Вы можете настроить получение событий системы Postfix в Kaspersky SIEM Cloud. Интеграция возможна только при отправке событий по syslog с использованием протокола TCP.

Система Postfix формирует события в двух форматах:

- Многострочные события, содержащие информацию о сообщениях (с уникальным идентификатором). События имеют следующий вид:

  ```
  <syslog PRI> время хост имя_процесса: идентификатор: информация из базового события 1
  <syslog PRI> время хост имя_процесса: идентификатор: информация из базового события 2
  ```

- Однострочные, содержащие информацию об ошибках (без идентификатора). События имеют следующий вид:

  ```
  <syslog PRI> время хост имя_процесса: критичность: основная информация для парсинга
  ```

Для обработки событий системы Postfix используется набор ресурсов Kaspersky SIEM Cloud, который необходимо применить при создании коллектора:

- Нормализатор.
- Правило агрегации.
- Фильтры для точек назначения.

В процессе работы коллектора многострочные базовые события будут агрегированы на основе идентификатора событий, нормализованы, и одно событие будет направлено в хранилище и коррелятор.

Агрегированное событие примет следующий вид:

Служебная информация из правила агрегации: идентификатор: информация из базового события 1, информация из базового события 2, информация из базового события n

После агрегации полученное событие будет направлено в этот же коллектор, где будет выполняться нормализации агрегированного события.

Алгоритм обработки события системы Postfix

Для обработки события системы Postfix был реализован следующий алгоритм:

1. Первичная нормализация.

   На этом этапе выполняется первичная нормализация базовых событий, которые начинаются с символа "<", поступивших по syslog. События приводятся к формату, пригодному для последующей агрегации: из события выделяется первый символ и размещается в поле FlexString1, идентификатор размещается в поле ExternalID, имя хоста размещается в поле DeviceHostName. Базовая нормализация выполняется в основном нормализаторе.

2. Проверка на агрегацию.

   Выполняется проверка является ли событие агрегированным или нет. В результате проверки к неагрегированным событиям (первый символ не "{" и идентификатор не пустой) применяется правило агрегации, а затем агрегированные события направляются на повторную нормализацию.

3. Применение правила агрегации.

   На этом этапе к событиям применяется правило агрегации, базовые события "склеиваются" и принимают следующий вид:

   Служебная информация из правила агрегации: идентификатор: информация из базового события 1, информация из базового события 2, информация из базового события n.

4. После выполнения агрегации "склеенное" событие направляется обратно в этот же коллектор для выполнения нормализации агрегированного события.

   Чтобы замкнуть цикл обработки события, следует указать тот же самый коллектор в качестве точки назначения. На схеме точка назначения названа "Loop", чтобы обозначить цикл обработки события. Вы можете назвать точку назначения произвольным именем.

5. Нормализация агрегированного события.

   Нормализация агрегированного события. начинающегося с символа "{", выполняется в экстранормализаторах Aggregated events, Aggregated events. Message KV parser, Aggregated events. Message regex 1, Aggregated events. Message regex 2.

6. Отправка в хранилище и коррелятор.

   Агрегированные и нормализованные события отправляются в хранилище и коррелятор.

На следующем рисунке представлена схема обработки событий от системы Postfix.

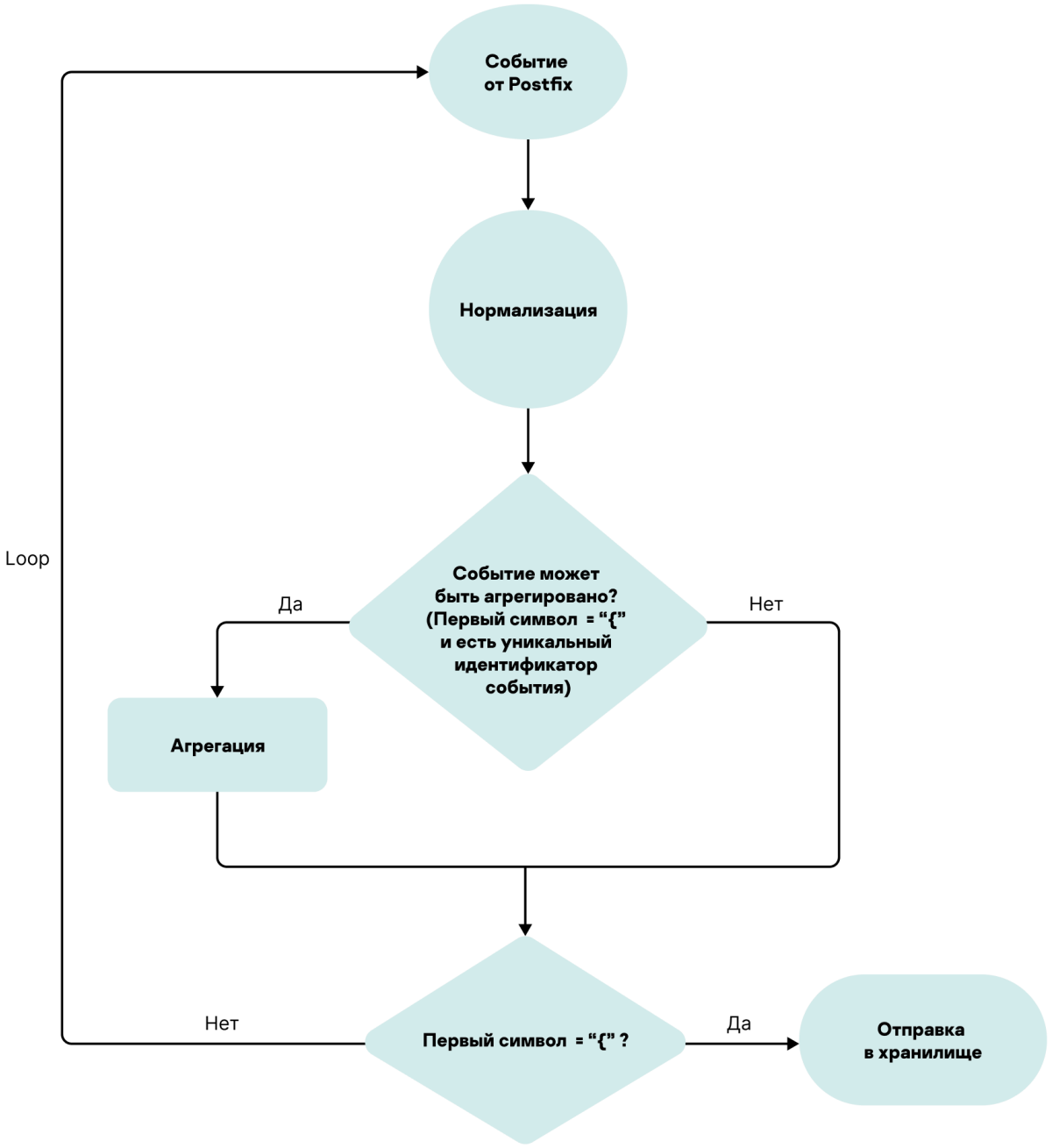


Схема обработки событий от системы Postfix

Настройка получения событий состоит из следующих этапов:

1. Настройка Postfix для отправки событий

События аудита системы Postfix по умолчанию направляются в файл `/var/log/maillog` или `/var/log/mail`.

1. Создайте резервную копию файла `/etc/rsyslog.conf`.

2. Откройте файл `/etc/rsyslog.conf` в режиме редактирования.

3. Добавьте в конец файла `/etc/rsyslog.conf` строку:

```
mail.* @@<Kaspersky SIEM Cloud collector IP address>:<Kaspersky SIEM Cloud collector port>
```

4. Сохраните файл `/etc/rsyslog.conf`.

5. Перезапустите сервис rsyslog с помощью команды:

```
sudo systemctl restart rsyslog
```

2 Создание коллектора Kaspersky SIEM Cloud для получения событий Postfix

1. Импортируйте пакет [OOTB] Postfix из репозитория Kaspersky SIEM Cloud.

2. Создайте новый коллектор и в мастере установки коллектора настройте следующие параметры:

   a. На шаге **Транспорт** в поле **Тип** выберите тип **tcp**, в поле **URL** укажите FQDN или IP-адрес и порт коллектора.

   b. На шаге **Парсинг событий** нажмите **Добавить парсинг событий** и в открывшемся окне **Основной парсинг событий** в раскрывающемся списке **Нормализатор** выберите нормализатор **[OOTB] Postfix syslog**.

   c. На шаге **Агрегация событий** нажмите **Добавить правило агрегации** и в открывшемся окне **Агрегация событий** в раскрывающемся списке **Правило агрегации** выберите правило агрегации **[OOTB] Postfix. Aggreation rule**.

   d. На шаге **Маршрутизация** нажмите **Добавить** и в открывшемся окне **Создание точки назначения** последовательно создайте три точки назначения: этот же коллектор с именем `Loop`, хранилище и коррелятор.

      1. Создайте точку назначения с именем `Loop` со следующими параметрами:

         - На вкладке **Основные параметры** в раскрывающемся списке Тип выберите тип транспорта **tcp**, в поле **URL** укажите FQDN или IP-адрес и порт коллектора, указанные ранее на шаге 2.1 этой инструкции.
         - На вкладке **Дополнительные параметры** в раскрывающемся списке **Фильтр** выберите фильтр **Postfix. Filter for event aggregation**.

      Настройка этих параметров необходима для отправки агрегированного события в тот же самый коллектор для дальнейшей нормализации.

      2. Создайте точку назначения коррелятора:

         - На вкладке **Основные параметры** в раскрывающемся списке **Тип** выберите **correlator** и заполните поле **URL**.
         - На вкладке **Дополнительные параметры** в раскрывающемся списке **Фильтр** выберите фильтр **Postfix. Aggregated events to storage and correlator**.

3. Создайте точку назначения хранилища:

   - На вкладке **Основные параметры** в раскрывающемся списке **Тип** выберите **storage** и заполните поле **URL**.
   - На вкладке **Дополнительные параметры** в раскрывающемся списке **Фильтр** выберите фильтр **Postfix. Aggregated events to storage and correlator**.

   Настройка этих параметров необходима для отправки агрегированного нормализованного события в хранилище и коррелятор.

3. Нажмите на кнопку **Создать**.

   Сервис коллектора создан с заданными параметрами в веб-интерфейсе Kaspersky SIEM Cloud. На экране отобразится команда для установки сервиса на сервере.

4. Скопируйте команду для установки коллектора Kaspersky SIEM Cloud.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Postfix требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❹ Проверка поступления событий Postfix в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий Postfix выполнена правильно, выполнив поиск связанных событий.

Sendmail

Настройка получения событий из почтового агента Sendmail Kaspersky SIEM Cloud состоит из следующих этапов:

❶ Настройка журналирования Sendmail

По умолчанию события системы Sendmail записываются в syslog.

Чтобы убедиться в правильности настройки журналирования:

1. Подключитесь по SSH к серверу, на котором установлена система Sendmail.
2. Выполните команду:

   ```
   cat /etc/rsyslog.d/50-default.conf
   ```

   Команда должна вернуть следующую строку:

   ```
   mail.* -/var/log/mail.log
   ```

Если журналирование настроено правильно, вы можете перейти к настройке передачи событий Sendmail.

❷ Настройка сервера источника событий

Для передачи событий от сервера, на котором установлен почтовый агент Sendmail, в коллектор Kaspersky SIEM Cloud используется сервис rsyslog.

Чтобы настроить передачу событий Sendmail в коллектор:

1. Подключитесь к серверу, на котором установлен Sendmail, под учетной записью с правами администратора.
2. В директории `/etc/rsyslog.d/` создайте файл `Sendmail-to-siem.conf` и добавьте в него строку:

   ```
   If $programname contains 'sendmail' then @<collector_IP>:<collector_port>
   ```

   Пример

   ```
   If $programname contains 'sendmail' then @192.168.1.5:1514
   ```

   Если вы хотите отправлять события по протоколу TCP, содержимое файла должно быть таким:

   ```
   If $programname contains 'sendmail' then @@<collector IP>:<collector_port>
   ```

   где:

   - `<collector_IP>` – IP-адрес коллектора.
   - `<collector_port>` – порт коллектора.
3. Создайте резервную копию файла `/etc/rsyslog.conf`.
4. В конфигурационный файл `/etc/rsyslog.conf` добавьте следующие строки:

   ```
   $IncludeConfig /etc/Sendmail-to-siem.conf
   $RepeatedMsgReduction off
   ```

5. Сохраните внесенные изменения.
6. Перезапустите сервис rsyslog, выполнив следующую команду:

   ```
   sudo systemctl restart rsyslog.service
   ```

❸ Создание коллектора Kaspersky SIEM Cloud

При создании коллектора в веб-интерфейсе Kaspersky SIEM Cloud в разделе **Парсинг событий** выберите нормализатор **[OOTB] Sendmail syslog** и в разделе **Транспорт** выберите тип коннектора **tcp** или **udp**.

❹ Установка коллектора Kaspersky SIEM Cloud

После завершения создания и настройки коллектора для сбора событий Sendmail требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

5. Проверка поступления событий Sendmail в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий Sendmail выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

VK WorkSpace Mail

Kaspersky SIEM Cloud позволяет осуществлять мониторинг событий системы VK WorkSpace Mail версии 1.23, поступающих в формате syslog в Kaspersky SIEM Cloud.

Настройка получения событий состоит из следующих этапов:

1. Настройка передачи событий VK WorkSpace Mail

Чтобы настроить передачу событий от VK WorkSpace Mail в Kaspersky SIEM Cloud:

1. В веб-интерфейсе VK WorkSpace Mail перейдите в раздел **Настройки дублирования действий пользователей во внешние хранилища**.
2. Установите флажок для параметра **Дублировать действия пользователей в syslog**.
3. В поле **Адрес сервера syslog** укажите IP-адрес или FQDN коллектора Kaspersky SIEM Cloud.
4. В поле **Порт сервера syslog** укажите порт, который прослушивает коллектор Kaspersky SIEM Cloud.
5. В поле **Протокол syslog, TCP или UDP** выберите протокол передачи данных.
6. В поле **Идентификатор данных syslog** укажите `bein`.

2. Создание коллектора Kaspersky SIEM Cloud для сбора событий VK WorkSpace Mail

Для получения событий аудита системы VK WorkSpace Mail при создании коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] VK WorkSpace Mail syslog**. Также на вкладке **Транспорт** нужно указать те же порт и протокол сервера syslog, что вы указали при настройке передачи событий VK WorkSpace Mail.

3. Установка коллектора в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий VK WorkSpace Mail требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

4. Проверка поступления событий VK WorkSpace Mail в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий VK WorkSpace Mail выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Прочие специализированные системы

В этом разделе описана настройка получения событий специализированных решений.

Codemaster Mirada

Вы можете настроить получение событий Codemaster Mirada в Kaspersky SIEM Cloud.

Настройка получения событий состоит из следующих этапов:

1 Настройка аудита системы Codemaster Mirada

Система Codemaster Mirada может отправлять события по протоколу Syslog.

1. Подключитесь к веб-интерфейсу системы Codemaster Mirada под учетной записью с правами администратора.
2. Перейдите в раздел **Настройки** → **Syslog**.
3. Включите сервис передачи событий, используя переключатель.
4. Выберите тип и формат протокола, нажав на кнопку со значком в виде точки, заключенной в круг.
5. В поле **Устройство** укажите IP-адрес коллектора Kaspersky SIEM Cloud.
6. В поле **Протокол** укажите транспортный протокол **UDP** или **TCP**.
7. В поле **Порт** укажите порт, который прослушивает коллектор Kaspersky SIEM Cloud.

   По умолчанию используется порт 514.
8. В поле **Формат** укажите стандарт **RFC 3164**.
9. Нажмите на кнопку **Сохранить** в нижней части веб-интерфейса, чтобы сохранить внесенные изменения.

2 Создание коллектора Kaspersky SIEM Cloud для получения событий Codemaster Mirada

Для получения событий Codemaster Mirada при создании коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] Codemaster Mirada syslog**, на шаге **Транспорт** выберите тип коннектора **tcp** или **udp**.

3 Установка коллектора в сетевой инфраструктуре

После завершения настройки коллектора для сбора событий Codemaster Mirada требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

4 Проверка поступления событий Codemaster Mirada в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка сервера источника событий Codemaster Mirada выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

АПКШ Континент

В поставку Kaspersky SIEM Cloud входит утилита kuma-kont, которая состоит из исполняемого файла и файла конфигурации. Утилита позволяет выполнить подключение к базе данных MSSQL, получать события АПКШ Континент и отправлять данные в коллектор Kaspersky SIEM Cloud в формате JSON. Импорт данных поддерживается для АПКШ Континент 3.9.2.

Список операционных систем, на которых поддерживается работа утилиты kuma-kont, приведен в разделе Программные требования.

Настройка сбора из базы данных MSSQL событий АПКШ Континент и их отправка в коллектор Kaspersky SIEM Cloud состоит из следующих этапов:

1. Создание коллектора Kaspersky SIEM Cloud для получения событий АПКШ Континент 3.9

При создании коллектора на шаге **Парсинг событий** выберите нормализатор **[OOTB] SecurityCode Continent 3.9 json**. Также на вкладке **Транспорт** требуется задать порт и протокол, указанные в конфигурационном файле kuma-kont-config.yaml в группе параметров KUMA Collector.

2. Установка коллектора в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий АПКШ Континент требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

3. Создание учетной записи в СУБД MSSQL

Создайте учетную запись в базе данных с минимально необходимым набором прав для подключения и чтения данных в таблицах: ALERTLOG, SERVERACCESSLOG, SYSTEMLOG, PACKETLOG, FILTERS.

4. Обеспечение сетевой связанности

Необходимо обеспечить сетевую связанность между сервером, на котором работает утилита, и сервером базы данных системы Континент, а также между сервером, на котором работает утилита и сервером коллектора Kaspersky SIEM Cloud.

5. **Создание конфигурационного файла kuma-kont-config.yaml**

1. Перейдите в директорию установщика Kaspersky SIEM Cloud, выполнив следующую команду:

```
cd kuma-ansible-installer/roles/kuma/files
```

2. Распакуйте архив kuma-kont.tar:

```
tar -xvf kuma-kont.tar
```

3. Перейдите в директорию с утилитой:

```
cd kuma-kont
```

4. Скопируйте шаблон kuma-kont-config-template.yaml и создайте конфигурационный файл с именем kuma-kont-config.yaml:

```
cp kuma-kont-config-template.yaml kuma-kont-config.yaml
```

5. Измените права на чтения для файла конфигурации:

```
sudo chown <user account>:<user account> kuma-kont-config.yaml
sudo chmod 600 kuma-kont-config.yaml
```

Замените `<учетная запись>` на имя пользователя операционной системы, от которого будет запускаться сервис.

6. Измените параметры конфигурационного файла `kuma-kont-config.yaml`.

Параметры конфигурационного файла kuma-kont-config.yaml

В таблице представлены параметры, доступные для настройки в файле kuma-kont-config.yaml.

Параметры конфигурационного файла kuma-kont-config.yaml

Параметр	Описание
`debug`	Необязательный параметр в группе **General settings**. Используется при необходимости вывода логов уровня отладки. При значении false, выводятся только сообщения о старте и завершении работы, а также ошибки, которые возникли в процессе отправки. Доступные значения: • **true** • **false** Значение по умолчанию: **false**.
`need_reconnect`	Необязательный параметр в группе **General settings**. Параметр определяет будет ли утилита выполнять переподключение к базе данных при каждом запросе. Доступные значения: • **true** • **false** Значение по умолчанию: **false**.
`state_file`	Обязательный параметр в группе **General settings**. Абсолютный путь к JSON-файлу, который используется для сохранения состояния обработанных логов. Файл создается автоматически по данному адресу. Убедитесь, что у пользователя достаточно прав на запись в эту директорию. Пример: /home/user/kuma-kont/state.json
`log_file_path`	Обязательный параметр в группе **General settings**. Абсолютный путь к файлу журналов для записи действий коннектора. Файл создается автоматически по данному адресу. Убедитесь, что у пользователя достаточно прав на запись в эту директорию. Пример: /home/user/kuma-kont/kuma-kont.log
`poll_interval`	Необязательный параметр в группе **General settings**. Интервал опроса базы данных. По умолчанию: 10 секунд При высоком потоке EPS мы не рекомендуем указывать значение выше 15 секунд.

Параметр	Описание
`name`	Обязательный параметр в группе **Kontinent Database**. Названия базы данных, в которую приходят журналы АПКШ.
`user`	Обязательный параметр в группе **Kontinent Database**. Имя пользователя базы данных.
`password`	Обязательный параметр в группе **Kontinent Database**. Пароль пользователя базы данных.
`host`	Обязательный параметр в группе **Kontinent Database**. URL сервера базы данных.
`port`	Обязательный параметр в группе **Kontinent Database**. Порт сервера базы данных. Убедитесь, что он доступен с сервера, на котором установлена утилита.
`limit`	Необязательный параметр в группе **Kontinent Database**. Ограничение по количеству выгружаемых событий из базы данных за один раз. По умолчанию 100_000 событий за один опрос базы данных. Мы не рекомендуем указывать меньшее значение при высоком потоке EPS.
`alert_log`	Необязательный параметр в группе **Last Id**. Указывает на событие типа AlertLog, с которого необходимо начать отправлять события в коллектор Kaspersky SIEM Cloud. Работает только при первом запуске или при отсутствии файла состояния. По умолчанию: 0
`packet_log`	Необязательный параметр в группе **Last Id**. Указывает на событие типа PacketLog, с которого необходимо начать отправлять события в коллектор Kaspersky SIEM Cloud. Работает только при первом запуске или при отсутствии файла состояния. По умолчанию: 0
`server_access_log`	Необязательный параметр в группе **Last Id**. Указывает на событие типа ServerAccessLog, с которого необходимо начать отправлять события в коллектор Kaspersky SIEM Cloud. Работает только при первом запуске или при отсутствии файла состояния. По умолчанию: 0
`system_log`	Необязательный параметр в группе **Last Id**. Указывает на событие типа SystemLog, с которого необходимо начать отправлять события в коллектор Kaspersky SIEM Cloud. Работает только при первом запуске или при отсутствии файла состояния. По умолчанию: 0
`address`	Обязательный параметр в группе **KUMA Collector**. Полное доменное имя (FQDN) или IP-адрес сервера, на котором установлен коллектор Kaspersky SIEM Cloud.
`port`	Обязательный параметр в группе **KUMA Collector**. Порт коллектора Kaspersky SIEM Cloud.
`protocol`	Обязательный параметр в группе **KUMA Collector**. Протокол передачи данных, который используется в коллекторе Kaspersky SIEM Cloud. Если используется протокол udp, повторная отправка событий при потере соединения с коллектором Kaspersky SIEM Cloud не будет осуществлена. Доступные значения: • **tcp** • **udp**

Необходимо задать значения для следующих параметров:

- параметры секции General settings: `state_file`, `log_file_path`.
- параметры секции Kontinent Database: `name`, `user`, `password`, `host`, port.
- параметры секции KUMA Collector: `address`, `port`, `protocol`.

7. Сохраните изменения в файле.

Конфигурационный файл будет создан.

6 Создание сервиса kuma-kont

1. Измените права на запуск для исполняемого файла:

```
sudo chown <user account>:<user account> <path to executable file>
sudo chmod 700 <path to executable file>
```

2. Создайте файл с именем `` `kuma-kont.service` `` в директории `/etc/systemd/system/` со следующим содержимым:

```
[Unit]
Description=Connector Kontinent 3.9
After=network.target
[Service]
User=<user account>
ExecStart=<path to executable file> --config <path to configuration file>
Restart=always
RestartSec=10
[Install]
WantedBy=multi-user.target
```

Замените `<учетная запись>` на имя пользователя операционной системы, от которого будет запускаться сервис.

3. Укажите путь к исполняемому файлу `` `kuma-kont` `` в поле `` `ExecStart` ``.

Например, если файл `` `kuma-kont` `` находится в директории `` `/usr/bin/` ``, то оставьте значение по умолчанию.

4. Укажите путь к конфигурационному файлу `` `kuma-kont-config.yaml` `` в поле `` `ExecStart` ``.

Например, если файл `` `kuma-kont-config.yaml` `` находится в директории `` `/path/to/` ``, то укажите этот путь.

Пример файла `kuma-kont.service`

```
[Unit]
Description=Continent Service
After=network.target
[Service]
User=user-example
ExecStart=./usr/bin/kuma-kont --config /path/to/kuma-kont-config.yaml
Restart=always
RestartSec=10
[Install]
WantedBy=multi-user.target
```

5. Загрузите конфигурацию менеджера systemd, выполнив команду:

```
sudo systemctl daemon-reload
```

6. Добавьте сервис в автозагрузку операционной системы, выполнив команду:

```
sudo systemctl enable kuma-kont
```

Утилита kuma-kont будет запускаться как сервис при загрузке системы.

7 Запуск утилиты kuma-kont

После активации утилита начнет выполнять экспорт событий из базы данных MSSQL и отправку в коллектор Kaspersky SIEM Cloud. Доступен журнал kuma-kont.log.

Для запуска сервиса утилиты выполните команду:

```
sudo systemctl start kuma-kont
```

Будет начат сбор событий из базы данных MSSQL и их отправка в коллектор Kaspersky SIEM Cloud.

Управление сервисом утилиты осуществляется с помощью следующих команд:

Запуск сервиса kuma-kont

```
sudo systemctl start kuma-kont
```

Остановка сервиса kuma-kont

```
sudo systemctl stop kuma-kont
```

Перезапуск сервиса kuma-kont

```
sudo systemctl restart kuma-kont
```

Также можно выполнить отправку событий с помощью утилиты kuma-kont, работающей как приложение. Чтобы начать отправку событий в коллектор Kaspersky SIEM Cloud выполните следующую команду, находясь в директории с исполняемым файлом:

```
./kuma-kont --config <file path kuma-kont-config.yaml>
```

Поведение при потере соединения

Соединение с базой данных MSSQL.

При потере соединения с базой данных MSSQL утилита будет пытаться восстановить соединение с ним каждые **n** секунд (где **n** – равно значению параметра `poll_interval`, конфигурационного файла), до тех пор, пока соединение не будет восстановлено.

Соединение с коллектором Kaspersky SIEM Cloud.

В случае использования протокола TCP для отправки событий при потере соединения с коллектором Kaspersky SIEM Cloud утилита также будет пытаться его восстановить. Интервал между попытками установить соединение будет увеличиваться до тех пор, пока не достигнет одного часа, затем попытка установить соединение будет выполняться один раз в час.

Известные ограничения

Не полностью расшифровывается событие из таблицы `AlertLog` со значением `"AL_CATEGORY" = 5`.

Ansible

Настройка получения событий от системы Ansible (версия 2.10.8), поступающих по протоколу Syslog в Kaspersky SIEM Cloud, состоит из следующих этапов:

1. Настройка передачи событий Ansible в Kaspersky SIEM Cloud

1. Проверьте, что на сервере источника событий установлен сервис rsyslog. Для этого выполните следующую команду под учетной записью с правами администратора:

   ```
   sudo systemctl status rsyslog.service
   ```

   Если сервис rsyslog не установлен на сервере, установите его, выполнив следующие команды:

   ```
   yum install rsyslog
   sudo systemctl enable rsyslog.service
   sudo systemctl start rsyslog.service
   ```

2. В директории `/var/log/` создайте директорию `ansible`.

3. В директории `/var/log/ansible` создайте файл `ansible.log`.

4. Перейдите в рабочую директорию Ansible.

   Пример

   ```
   cd ~/ansible-playbooks/
   ```

5. Создайте или измените конфигурационный файл Ansible:

   ```
   sudo nano ansible.cfg
   ```

   Файл `ansible.cfg` должен выглядеть следующим образом:

   ```
   [defaults]
   log_path = /var/log/ansible/ansible.log
   log_level = INFO
   inventory = <inventory file or path to the inventory file>
   ```

6. Перейдите в директорию `/etc/rsyslog.d/` и создайте файл `ansible-to-siem.conf`.

7. В конфигурационный файл `/etc/rsyslog.d/ansible-to-siem.conf` добавьте следующие строки:

```
module(load="imfile")

input(type="imfile"
    File="/var/log/ansible/ansible.log"
    Tag="tag_Ansible_log:"
    facility="local1"
    Startmsg.regex="^[0-9]{4}-[0-9]{2}-[0-9]{2} [0-9]{2}:[0-9]{2}:[0-9]{2},[0-9]{3}"
)

template(name="Ansible_log" type="string"
    string="<%pri%>%timegenerated% %HOSTNAME% %syslogtag% %msg%\n"
)

if $syslogtag startswith 'tag_Ansible_log:' then {
    action(type="omfwd"
           target="<Kaspersky SIEM Cloud collector IP address>"
           port="<Kaspersky SIEM Cloud collector port>"
           protocol="<udp or tcp>"
           template="Ansible_log")
stop
}
```

Если значение параметра `facility local1` уже используется другой программой на сервере, измените значение параметра `facility` для Ansible на другое значение.

8. Сохраните изменения в конфигурационном файле `/etc/rsyslog.d/ansible-to-siem.conf`.

9. В конфигурационный файл `/etc/rsyslog.conf` добавьте следующие строки:

```
$IncludeConfig /etc/rsyslog.d/ansible-to-siem.conf
$RepeatedMsgReduction off
```

10. Сохраните изменения в конфигурационном файле `/etc/rsyslog.conf`.

11. Перезапустите сервис rsyslog:

```
sudo systemctl restart rsyslog.service
```

Система Ansible не выполняет ротацию журналов. Чтобы снизить риск переполнения дискового пространства, рекомендуется использовать внешние инструменты ротации журналов, например Logrotate или Logadm.

❷ Создание коллектора Kaspersky SIEM Cloud для получения событий Ansible

При создании коллектора в Kaspersky SIEM Cloud на шаге **Парсинг событий** выберите нормализатор **[OOTB] Ansible syslog**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Ansible требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

4 Проверка поступления событий Ansible в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что поступление событий из Ansible настроено правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Grafana

Настройка получения событий аудита от системы Grafana (версии 9.5.15) в Kaspersky SIEM Cloud состоит из следующих этапов:

1 Настройка аудита и отправки событий Grafana в Kaspersky SIEM Cloud

1. Откройте конфигурационный файл `/etc/grafana/grafana.ini` и измените значения следующих параметров:

```
mode = syslog
     level = info
```

2. Измените значения следующих параметров в зависимости от используемого протокола:

Для отправки событий по протоколу UDP

```
level = info
format = json
network = udp
address = "<Kaspersky SIEM Cloud collector IP address>:<Kaspersky SIEM Cloud collector port>
tag = Grafana
```

Для отправки событий по протоколу TCP

```
level = info
format = json
network = tcp
address = "<Kaspersky SIEM Cloud collector IP address>:<Kaspersky SIEM Cloud collector port>"
tag = Grafana
```

3. Перезапустите службу Grafana:

```
systemctl restart grafana-server
```

2 Создание коллектора Kaspersky SIEM Cloud для получения событий Grafana

При создании коллектора в Kaspersky SIEM Cloud на шаге **Транспорт** укажите те же порт и протокол, которые вы указали при настройке отправки событий Grafana. Для получения событий из Grafana на шаге **Парсинг событий** выберите нормализатор **[OOTB] Grafana json**.

3 Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий Grafana требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

4 Проверка поступления событий Grafana в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что поступление событий из Grafana настроено правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

TeamPass

Перед настройкой убедитесь, что таблицы базы данных TeamPass имеют префикс **«teampass_»**. Если префикс другой, то необходимо изменить название таблиц в запросах коннектора **[OOTB] TeamPass MySQL** на название, используемое в вашем экземпляре.

Настройка получения событий системы TeamPass (версия 3.1) из БД MySQL в Kaspersky SIEM Cloud состоит из следующих этапов:

1 Создание учетной записи в MySQL

Настройку передачи событий требуется выполнять под учетной записью с минимально необходимым набором прав для подключения и чтения данных в таблицах.

1. Запустите командную строку на сервере, где установлен MySQL.
2. Авторизуйтесь в СУБД под учетной записью администратора:

   ```
   mysql --user=root --password=<password> --database=<database name>
   ```

3. Создайте учетную запись:

   ```
   CREATE USER <login> IDENTIFIED BY '<password>';
   ```

4. Предоставьте учетной записи права на чтение БД:

   ```
   GRANT SELECT ON <database>.* TO <login>;
   ```

5. Примените изменения:

   ```
   FLUSH PRIVILEGES;
   EXIT
   ```

   Учетная запись создана.

6. Проверьте доступ к базе данных, выполнив следующие действия:

   a. Запустите командную строку на сервере, где установлен MySQL.

   b. Определите порт подключения к СУБД:

   ```
   mysql --user=root --password=<password> -e "SHOW VARIABLES LIKE 'port';"
   ```

   Порт по умолчанию 3306.

   c. Выполните запрос к базе данных под новой учетной записью:

   ```
   mysql -h <server> --user=<login> --password=<password> -P <port> <database name> -e "SELECT ls.id AS id, ls.type AS category, ls.date AS date, ls.label AS action, ls.qui AS suser_id, ls.field_1 AS duser_id, tu1.login AS suser, tu2.login AS duser FROM teampass_log_system AS ls LEFT JOIN teampass_users tu1 ON ls.qui = tu1.id LEFT JOIN teampass_users tu2 ON ls.field_1 = tu2.id ORDER BY ls.id"
   ```

При наличии доступа к базе данных на экране отобразится результат запроса.

2 Создание секрета

После создания и настройки учетной записи в MySQL требуется добавить секрет в веб-интерфейсе Kaspersky SIEM Cloud. Этот ресурс используется для хранения учетных данных для подключения к MySQL.

1. В веб-интерфейсе откройте раздел **Ресурсы** → **Секреты**.

   Отобразится список доступных секретов.

2. Выберите секрет **[OOTB] TeamPass MySQL**.

   Откроется окно секрета

3. В поле **URL** укажите строку вида:

   ```
   mysql://<user>:<password>@tcp(<server>:<port>)/<database>
   ```

   где:

   - `user` – имя созданной учетной записи MySQL с правами для подключения и работы с базой данных.
   - `password` – пароль созданной учетной записи MySQL.
   - `server` – имя или IP-адрес сервера с базой данных MySQL.
   - `database_name` – имя базы данных TeamPass.

   Пример

   ```
   mysql://user:password@tcp(teampass.example.com:3306)/teampass_db
   ```

   Если в пароле учетной записи MS SQL используются специальные символы (@ # $ % & * ! + = [ ] : ' , ? / \ ` ( ) ;), переведите их в формат URL.

4. Нажмите **Сохранить**.

Для безопасности после сохранения секрета строка, указанная в поле URL, скрывается.

❸ Создание коллектора Kaspersky SIEM Cloud для получения событий **TeamPass**

При создании коллектора в Kaspersky SIEM Cloud на шаге **Транспорт** выберите коннектор **[OOTB] TeamPass MySQL**, на шаге **Парсинг событий** выберите нормализатор **[OOTB] TeamPass SQL**.

❹ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для получения событий TeamPass требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

❺ Проверка поступления событий из **TeamPass** в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что настройка поступления событий из TeamPass выполнена правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

SaltStack

Настройка получения событий от системы SaltStack (версия 3004.1), поступающих по протоколу Syslog в Kaspersky SIEM Cloud, состоит из следующих этапов:

❶ Настройка передачи событий SaltStack в Kaspersky SIEM Cloud

1. Проверьте, что на сервере источника событий установлен сервис rsyslog. Для этого выполните следующую команду под учетной записью с правами администратора:

   ```
   sudo systemctl status rsyslog.service
   ```

   Если сервис rsyslog не установлен на сервере, установите его, выполнив следующие команды:

   ```
   yum install rsyslog
   sudo systemctl enable rsyslog.service
   sudo systemctl start rsyslog.service
   ```

2. Перейдите в директорию `/etc/rsyslog.d/` и создайте файл `saltstack-to-siem.conf`.

3. Для отправки событий добавьте в конфигурационный файл `/etc/rsyslog.d/saltstack-to-siem.conf` следующие строки в зависимости от используемого протокола:

   - Для отправки событий по протоколу UDP:

     ```
     if $programname == 'salt-master' or $programname == 'salt-minion' then @<collector IP address>:<collector port>
     ```

     Пример

     ```
     if $programname == 'salt-master' or $programname == 'salt-minion' then @192.168.1.5:1514
     ```

   - Для отправки событий по протоколу TCP:

     ```
     if $programname == 'salt-master' or $programname == 'salt-minion' then @@<collector IP address>:<collector port>
     ```

     Пример

     ```
     if $programname == 'salt-master' or $programname == 'salt-minion' then @@192.168.1.5:1514
     ```

4. Сохраните изменения в конфигурационном файле `saltstack-to-siem.conf`.

5. В конфигурационный файл `/etc/rsyslog.conf` добавьте следующие строки:

   ```
   $IncludeConfig /etc/rsyslog.d/saltstack-to-siem.conf
   $RepeatedMsgReduction off
   ```

6. Сохраните изменения в конфигурационном файле `/etc/rsyslog.conf`.

7. Перезапустите сервис rsyslog:

   ```
   sudo systemctl restart rsyslog.service
   ```

❷ Создание коллектора Kaspersky SIEM Cloud для получения событий SaltStack

При создании коллектора в Kaspersky SIEM Cloud на шаге **Парсинг событий** выберите нормализатор **[OOTB] SaltStack syslog**.

❸ Установка коллектора Kaspersky SIEM Cloud в сетевой инфраструктуре

После завершения создания и настройки коллектора для сбора событий SaltStack требуется установить коллектор Kaspersky SIEM Cloud на сервере сетевой инфраструктуры, предназначенной для получения событий.

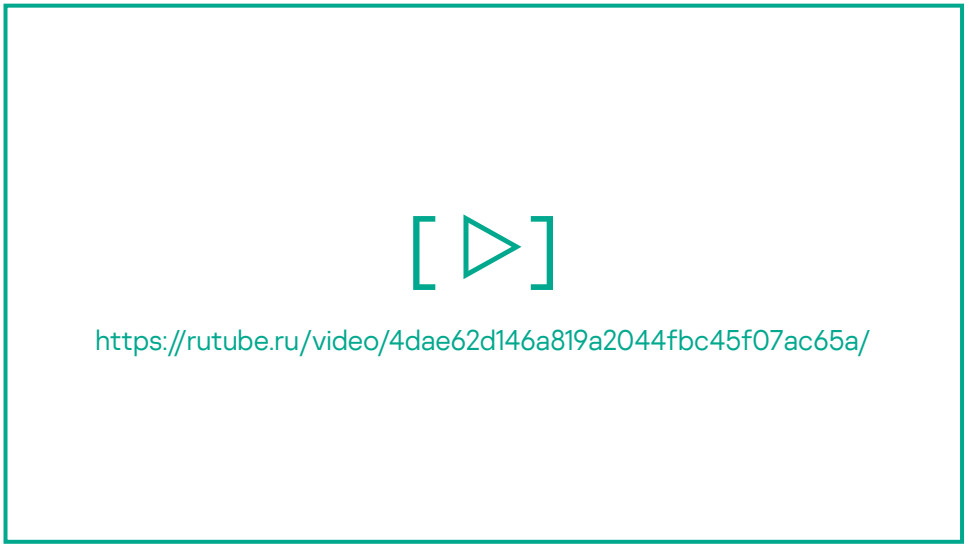
❹ Проверка поступления событий SaltStack в коллектор Kaspersky SIEM Cloud

Вы можете проверить, что поступление событий из SaltStack настроено правильно, выполнив поиск связанных событий в веб-интерфейсе Kaspersky SIEM Cloud.

Мониторинг источников событий

В организации может быть множество различных источников событий: контроллеры доменов, серверы Kaspersky Security Center, рабочие станции под защитой Kaspersky Endpoint Security. Если какой-то источник перестает передавать события в Kaspersky SIEM Cloud, возникает угроза информационной безопасности. Нужно отслеживать прекращение потока событий от источников и отправлять уведомления о таких ситуациях администраторам систем.

Для наглядного ознакомления с мониторингом источников событий вы можете просмотреть видео ниже.



https://rutube.ru/video/4dae62d146a819a2044fbc45f07ac65a/

Способы настроить мониторинг источников событий

По умолчанию Kaspersky SIEM Cloud определяет источник события по полям `DeviceProduct`, `DeviceHostName`, `DeviceAddress`, `DeviceProcessName`. Эти данные отображаются в названии источника событий. При необходимости можно вручную указать поля, по которым определяются источники событий.

Для контроля потока событий, поступающих от источника (например, для автоматического отслеживания, когда поток событий стал аномально большим, слишком слабым или прекратился), к источнику событий можно применить *политику мониторинга*. По умолчанию в решении созданы три политики мониторинга: High bounds policy, Low bounds policy и Middle bounds policy. Вы также можете создать дополнительные политики мониторинга.

В политике можно указать нижнее и верхнее пороговые значения, а также способ отслеживать события: по частоте (EPS) или по количеству. При достижении индикаторами значений, указанных в параметрах примененной политики мониторинга, создается событие мониторинга с данными об источнике событий и отправляется уведомление на электронную почту. К источнику событий можно применить одну или несколько политик мониторинга.

Политики мониторинга отображаются в веб-консоли в разделе **Мониторинг → Состояние источников** на вкладке **Политики мониторинга**.

Инструменты мониторинга источников событий

Состояние источников можно контролировать несколькими способами:

- Список источников событий.

  Kaspersky SIEM Cloud позволяет контролировать состояние источников, данные из которых поступают в коллекторы. В коллекторах формируются списки источников, которые затем объединяются в Ядре Kaspersky SIEM Cloud и отображаются в веб-консоли в разделе **Мониторинг** → **Состояние источников** на вкладке **Список источников событий**. Информация об источниках событий обновляется каждую минуту.

  Состояние каждого источника вы можете отслеживать по его статусу. Статус источника определяется параметрами политики мониторинга, назначенной этому источнику.

- Уведомления на электронную почту.

  При срабатывании политики мониторинга на электронную почту будет приходить уведомление об этом. Настроить отправку уведомлений можно при создании или изменении политики мониторинга.

- Виджеты и отчеты.

  Если поток событий от источника выходит за пределы значений, указанных в политике мониторинга, Kaspersky SIEM Cloud создает информационное событие мониторинга потоков типа 5 (`Type=5`). Вы можете указать этот тип события в запросе, чтобы найти такие события в базе данных:

  ```
  SELECT * FROM 'events' WHERE Type=5
  ```

  На основе этого критерия поиска вы можете создавать виджеты типа **События** для визуализации состояния источников на панели мониторинга. Созданные виджеты можно добавить в шаблон отчета и настроить регулярную отправку отчета на электронную почту.

- Алерты.

  Вы можете создать правило корреляции, которое будет срабатывать при создании события мониторинга (`Type=5`), и привязать это правило к коррелятору. В таком случае при создании события мониторинга будет создаваться алерт.

Пример настройки мониторинга источников событий

Настройка мониторинга источников событий в инфраструктуре с контроллерами доменов, серверами Kaspersky Security Center и рабочими станциями состоит из следующих этапов:

1. **Создание политик мониторинга**

   Создайте политики мониторинга для контроллеров доменов, серверов Kaspersky Security Center и рабочих станций.

   Для контроллеров доменов укажите минимальный поток событий: 100 событий в секунду.

   Для серверов Kaspersky Security Center укажите минимальный поток событий: 100 событий в час.

   Для рабочих станций укажите минимальный поток событий: 1 событие в час. Также включите переключатель **Настроить расписание по дням недели** и укажите только будние дни.

2. **Настройка уведомлений**

   Для каждой политики укажите адрес электронной почты для отправки уведомлений, а также шаблон уведомлений.

3. **Включение политик мониторинга для источников событий**

   Назначьте каждому источнику событий соответствующую политику мониторинга.

Сформируется список источников событий. Для каждого из источников выполняется индивидуальный мониторинг потока событий. Например, если в Kaspersky SIEM Cloud перестанут поступать данные от контроллера домена, администратор получит уведомление на адрес электронной почты, а в хранилище Kaspersky SIEM Cloud будет отправлено информационное событие мониторинга потоков типа 5 (`Type=5`). Для отслеживания таких событий можно создавать виджеты, отчеты и алерты.

Состояние источников

В Kaspersky SIEM Cloud можно контролировать состояние источников, из которых поступают данные в коллекторы. На одном сервере может быть несколько источников событий, а данные из нескольких источников могут поступать в один коллектор.

Вы можете настроить автоматическое определение источников событий, используя один из следующих наборов полей:

- Пользовательский набор полей. Вы можете указать от 1 до 9 полей в желаемой последовательности. TenantID отдельно задавать не нужно, определяется автоматически.

- **Применить сопоставление по умолчанию**: DeviceProduct, DeviceHostName, DeviceAddress, DeviceProcessName. Порядок полей не подлежит изменению.

  Определение источников происходит, если следующие поля в событиях содержат непустые значения: DeviceProduct + DeviceAddress и/или DeviceHostname + TenantID (отдельно задавать это поле не нужно, определяется автоматически). Поле DeviceProcessName может содержать пустое значение. Если поле DeviceProcessName содержит непустое значение, и остальные обязательные поля заполнены, будет определен новый источник.

Определение источников событий в зависимости от наличия непустых значений в полях событий

DeviceProduct	DeviceHostName	DeviceAddress	DeviceProcessName	TenantID (определяется автоматически)	
+	+			+	Определятся источник 1
+		+		+	Определятся источник 2
+	+	+		+	Определятся источник 3
+	+		+	+	Определятся источник 4
+		+	+	+	Определятся источник 5
+	+	+	+	+	Определятся источник 6
	+	+		+	Источник не определяется
	+		+	+	Источник не определяется

DeviceProduct	DeviceHostName	DeviceAddress	DeviceProcessName	TenantID (определяется автоматически)	
		+	+	+	Источник не определяется
+			+	+	Источник не определяется

Применяется только один набор полей для всей инсталляции. При обновлении на новую версию Kaspersky SIEM Cloud применяется набор полей по умолчанию. Настраивать набор полей для определения источника событий может только пользователь с ролью Главный администратор. После того как вы сохраните изменения в наборе полей, ранее определенные источники событий будут удалены из веб-интерфейса Kaspersky SIEM Cloud и из базы данных. При необходимости вы можете вернуться к использованию набора полей для определения источников событий по умолчанию. Чтобы измененные параметры вступили в силу и Kaspersky SIEM Cloud начала определять источники с учетом новых параметров, перезапустите коллекторы.

Чтобы определить источники событий:

1. В веб-консоли перейдите в раздел **Мониторинг** → **Состояние источников**.
2. На вкладке **Список источников событий** в меню ⋮ нажмите **Настройки**.
3. В открывшемся окне **Настройки определения источников** в раскрывающемся списке **Группирующие поля для определения источника** выберите поля событий, по которым вы хотите определять источники событий.

   Вы можете указать до девяти полей в нужной последовательности. В пользовательской конфигурации Kaspersky SIEM Cloud определяет источники, в которых заполнено поле TenantID (отдельно задавать это поле не нужно, определяется автоматически) и хотя бы одно поле из указанных в списке **Группирующие поля для определения источника**. Для числовых полей 0 является пустым значением. Если для определения источников выбрано одно числовое поле и значение числового поля равно 0, источник не будет определен.

   После того, как вы сохраните измененный набор полей, будет создано событие аудита и все ранее определенные источники будут удалены из веб-интерфейса Kaspersky SIEM Cloud и из базы данных, назначенные политики будут отключены.
4. Если вы хотите вернуться к списку полей для определения источника событий по умолчанию, нажмите **Применить сопоставление по умолчанию**. Порядок полей по умолчанию не подлежит изменению. Если вы вручную укажете поля в неверном порядке, появится ошибка и кнопка сохранения настроек будет недоступна. Корректная последовательность полей по умолчанию: `DeviceProduct`, `DeviceHostName`, `DeviceAddress`, `DeviceProcessName`. Минимальная конфигурация для определения источников событий с использованием набора событий по умолчанию: непустые значения в полях событий `DeviceProduct` + `DeviceAddress` и/или `DeviceHostname` + `TenantID` (определяется автоматически).
5. Нажмите **Сохранить**.
6. Перезапустите коллекторы, чтобы изменения вступили в силу и источники событий начали определяться по заданному списку полей.

Настройка определения источников выполнена.

Чтобы просмотреть события, которые относятся к источнику событий:

1. В веб-консоли перейдите в раздел **Мониторинг → Состояние источников**.

2. На вкладке **Список источников событий** выберите в списке нужный источник событий и в столбце **Название** разверните меню для выбранного источника событий, нажмите на кнопку **событий за <количество> дней**.

   Kaspersky SIEM Cloud выполнит переход в раздел **Поиск угроз**, где вы сможете просмотреть список событий для выбранного источника за последние 5 минут. В запросе автоматически будут указаны значения полей, заданных в параметрах определения источника событий. При необходимости в разделе **Поиск угроз** можно изменить в запросе временной интервал и нажать **Выполнить запрос** повторно, чтобы просмотреть выборку за указанный промежуток времени.

Ограничения

1. В конфигурации с использованием набора полей по умолчанию Kaspersky SIEM Cloud регистрирует источник событий при условии, что поля DeviceProduct + DeviceAddress и\или DeviceHostName содержатся в сыром событии.

   Если сырое событие не содержит поля DeviceProduct + DeviceAddress и\или DeviceHostName, вы можете выполнить следующие действия:

   - Настроить обогащение в нормализаторе: на вкладке нормализатора **Обогащение** выберите тип данных **Событие**, укажите значения для параметра **Исходное поле**, для параметра **Целевое поле** выберите DeviceProduct + DeviceAddress и\или DeviceHostName и нажмите OK.

   - Использовать правило обогащения: выберите тип источника данных **Событие**, укажите значения для параметра **Исходное поле**, для параметра **Целевое поле** выберите DeviceProduct + DeviceAddress и\или DeviceHostName и нажмите **Создать**. Созданное правило обогащения необходимо привязать к коллектору на шаге Обогащение событий.

   Kaspersky SIEM Cloud выполнит обогащение и зарегистрирует источник событий.

2. Если в Kaspersky SIEM Cloud поступают события с одинаковыми значениями полей, определяющих источник, Kaspersky SIEM Cloud регистрирует разные источники при следующих условиях:

   - Значения обязательных полей совпадают, но для событий определяются разные тенанты.

   - Значения обязательных полей совпадают, но для одного из событий указано необязательное поле DeviceProcessName.

   - Значения обязательных полей совпадают, но у данных в этих полях не совпадает регистр.

Если вы хотите, чтобы Kaspersky SIEM Cloud регистрировала для таких событий один источник, вы можете дополнительно настроить поля в нормализаторе.

Списки источников формируются в коллекторах, объединяются в Ядре Kaspersky SIEM Cloud и отображаются в веб-консоли в разделе **Мониторинг → Состояние источников** на вкладке **Состояние источников**. Данные обновляются ежеминутно.

Данные о частоте и количестве поступающих событий являются важным показателем состояния наблюдаемой системы. Вы можете настроить политики мониторинга, чтобы изменения отслеживались автоматически и при достижении индикаторами определенных граничных значений автоматически создавались уведомления. Политики мониторинга отображаются в веб-консоли в разделе **Мониторинг** → **Состояние источников** на вкладке **Политики мониторинга**.

При срабатывании политик мониторинга создаются события мониторинга с данными об источнике событий.

Алгоритм применения политик мониторинга

Политики мониторинга применяются к источнику события по следующему алгоритму:

1. Поток событий подсчитывается на коллекторе.
2. Сервер Ядра Kaspersky SIEM Cloud с интервалом в 15 секунд собирает от коллекторов информацию о потоке.
3. Собранные данные сохраняются на сервере Ядра Kaspersky SIEM Cloud в СУБД временных рядов Victoria Metrics. Глубина хранения данных на сервере Ядра Kaspersky SIEM Cloud составляет 15 дней.
4. Один раз в минуту выполняется инвентаризация источников событий.
5. Поток подсчитывается отдельно для каждого источника событий по следующим правилам:
   - Если к источнику событий применяется политика мониторинга, то отображаемое максимальное число потока событий считается в соответствии с работающими в текущий момент политиками мониторинга за период, указанный в политике.

     В зависимости от типа политики число потока событий подсчитывается по количеству событий (для типа политики **количество поступивших событий** или для политик разных типов) или по количеству событий в секунду (EPS, для политики типа **частота поступления событий**). Вы можете узнать, в чем считается поток для назначенной политики, в столбце **Поток** на странице **Список источников событий**.
   - Если к источнику событий не применяется политика мониторинга, число потока событий отображает последнее значение.
6. Один раз в минуту проверяется, есть ли политики мониторинга, которые должны примениться к источникам событий или остановиться в соответствии с расписанием политики мониторинга.
7. Один раз в минуту поток событий проверяется на соответствие параметрам политики.

Если поток событий от источника выходит за пределы значений, указанных в политике мониторинга, информация об этом будет зафиксирована следующим образом:

- Уведомление о срабатывании политики мониторинга отправляется на адреса электронной почты, указанные в политике. Для каждой политики вы также можете задать шаблон уведомления.
- Формируется информационное событие мониторинга потоков типа `5` (`Type=5`). Событие содержит поля, описанные в таблице ниже.

Поля события мониторинга

Название поля события	Значение поля
`ID`	Уникальный идентификатор события.
`Timestamp`	Время события.

Название поля события	Значение поля
`Type`	Тип события аудита. Событию аудита соответствует значение `5` (мониторинг).
`Name`	Имя политики мониторинга.
`DeviceProduct`	`KUMA`
`DeviceCustomString1`	Значение из поля `value` в уведомлении. Отображает значение метрики, по которой отправлено уведомление.

Сформированное событие мониторинга отправляется в следующие ресурсы:

- все хранилища тенанта Main;
- все корреляторы тенанта Main;
- все корреляторы тенанта, в котором находится источник событий.

Хранение событий

Хранилище Kaspersky SIEM Cloud – сервис, который предназначен для хранения нормализованных событий и быстрого доступа к ним для извлечения аналитических данных. Хранилище представляет собой кластер ClickHouse, связанный с сервисом хранилища и остальными сервисами Kaspersky SIEM Cloud. Сервис хранилища получает данные от коллекторов и корреляторов, передает их в ClickHouse и позволяет настроить параметры хранения данных.

Встроенные механизмы ClickHouse обеспечивают кластеризацию базы данных, перенос данных между горячим и холодным хранилищами, а также архивирование данных. Кластеры ClickHouse можно дополнять дисками холодного хранения данных.

Нормализованные события хранятся на серверах облачной инфраструктуры, на которых развернут кластер узлов ClickHouse. После создания рабочей области и развертывания решения в соответствии с типовой конфигурацией вам доступно хранилище [OOTB] OSMP Storage. При развертывании решения размер хранилища [OOTB] OSMP Storage определяется таким образом, чтобы обеспечить хранение событий приблизительно 30 дней. При эксплуатации решения это значение может меняться, так как поток событий от источников в организации может меняться как в меньшую, так и в большую сторону. При заполнении хранилища самые старые данные автоматически удаляются.

Если вам нужно увеличить объем хранилища, вы можете создать ресурс дополнительного хранилища и развернуть дополнительный сервис хранилища. Дополнительные сервисы вы можете разворачивать только при достаточном количестве доступных вычислительных единиц.

Данные хранятся и удаляются из хранилища в соответствии с параметрами, указанными в свойствах хранилища. Вы можете изменить параметры хранения как для предустановленного хранилища [OOTB] OSMP Storage, так и для дополнительного хранилища. Отдельно вы можете настроить параметры хранения алертов и инцидентов.

Следующие параметры хранения предопределены, изменить их нельзя:

- Срок хранения событий, связанных с алертами и инцидентами: 30 дней.
- Запросы к сторонним ИИ-сервисам не сохраняются.
- Ответы ИИ-сервисов хранятся в кеше не более 14 дней.

В хранилищах можно создавать *пространства* для организации структуры данных, например для совместного хранения событий определенного типа.

Рекомендации по использованию системной памяти

Если вы создаете хранилище в системах с ограниченным объемом памяти и хотите регулировать потребление памяти, рекомендуется определить объем используемой памяти и увеличить значение параметра `max_server_memory_usage`. Этот параметр определяет максимальный объем памяти, который может использовать сервер. Значение указывается в байтах.

По умолчанию для `max_server_memory_usage` указано значение `0`. В этом случаем сервер может использовать всю доступную память.

Значение параметра `max_server_memory_usage` дополнительно ограничивается переменной `max_server_memory_usage_to_ram_ratio`, определяющей отношение используемой памяти ко всей доступной памяти. Например, значение 0,9 означает, что сервер может использовать до 90% доступной памяти.

При определении объема используемой памяти учитывайте следующие ограничения:

- Оптимальный объем памяти, доступный хранилищу, составляет около 75% общего объема системной памяти.

  > Не рекомендуется использовать 100% доступной памяти, так как это может привести к нехватке памяти при обработке поступающих запросов.

- Если на сервере установлены другие приложения, требуется выделить память для их работы.
- При изменении аппаратных параметров сервера, на котором развернуто хранилище, нужно скорректировать значения параметров использования памяти.

О кластере ClickHouse

Кластер ClickHouse – логическая группа устройств, включающая в себя шарды, реплики и киперы, которые совместно обеспечивают хранение всех нормализованных событий Kaspersky SIEM, их репликацию и координацию работы кластера. Кластер может включать один или несколько *шардов*.

Шард – логическая группа устройств, содержащих **часть** всех накопленных в кластере нормализованных событий. Увеличение количества шардов позволяет:

- Накапливать больше событий за счет увеличения общего количества серверов и дискового пространства.
- Обрабатывать больший поток событий за счет распределения нагрузки при записи новых событий.
- Уменьшать время поиска событий за счет распределения поисковых зон между несколькими устройствами.

Шард может включать одну или несколько *реплик.*

Реплика – устройство, входящее в состав шарда и содержащее копию его данных. Если реплик несколько, то копий тоже будет несколько (данные реплицируются). Увеличение количества реплик позволяет:

- Повысить отказоустойчивость.
- Распределить нагрузку, связанную с поиском данных, между несколькими устройствами.

Кипер – устройство, участвующее в координации репликации данных на уровне всего кластера. Для кластера требуется как минимум один кипер. Количество киперов должно быть нечетным. Рекомендуется использовать три устройства с ролью кипера. Роли кипера и реплики можно совмещать.

Перед созданием узлов кластера ClickHouse убедитесь в наличии сетевой связности между компонентами системы и откройте необходимые сетевые порты.

Изменение хранилища

В Kaspersky SIEM Cloud есть предустановленное хранилище [OOTB] OSMP Storage. Вы можете изменять параметры этого хранилища и добавлять в него свободное пространство. Новое хранилище создать нельзя.

Чтобы изменить параметры набора ресурсов для хранилища:

1. В разделе **Мониторинг** → **Ресурсы и сервисы** → **Хранилища** выберите хранилище [OOTB] OSMP Storage.

   Откроется окно **Изменение хранилища**.

2. На вкладке **Основные параметры** в поле **Название хранилища** введите уникальное имя создаваемого сервиса. Имя должно содержать от 1 до 128 символов в кодировке Unicode.

3. В поле **Тенант** отображается тенант, которому будет принадлежать хранилище. Изменить его нельзя.

4. В раскрывающемся списке **Теги** выберите теги для создаваемого набора ресурсов.

   В списке отображаются все доступные теги, созданные в тенанте ресурса и Общем тенанте. Вы может найти тег в списке, начав вводить его название в поле. Если тега, который вы ввели, не существует, вы можете нажать **`Enter`** или **Добавить**, чтобы создать его.

5. В поле **Описание** добавьте описание сервиса. Описание может содержать от 1 до 256 символов в кодировке Unicode.

6. В поле **Варианты условий хранения** выберите для хранилища условие хранения событий в кластере ClickHouse, при выполнении которого события будут переноситься на диски холодного хранения или удаляться, если холодное хранение не настроено или настроено неверно, начиная с партиций за самую старую дату.

   Условие будет применено к пространству по умолчанию и к событиям из удаленных пространств.

   По умолчанию ClickHouse перемещает события на диски холодного хранения или удаляет их, если заполнено более 97% хранилища. В Kaspersky SIEM Cloud при создании хранилища также используется дополнительное условие хранения **365 дней**.

   Чтобы задать условие хранения, выполните одно из следующих действий:

   - Если вы хотите ограничить срок хранения событий, в раскрывающемся списке выберите **Дни** и в поле укажите максимальный срок хранения событий в днях в кластере горячего хранилища ClickHouse.

     Минимальное значение – 1. Значение по умолчанию – 365.

- Если вы хотите ограничить максимальный размер хранилища, в раскрывающемся списке выберите **ГБ** и в поле укажите максимальный размер хранилища в гигабайтах.

  Минимальное значение и значение по умолчанию – 1 ГБ.

- Если вы хотите ограничить размер хранилища относительно объема диска, который доступен хранилищу, в раскрывающемся списке выберите **Проценты** и укажите максимальный размер хранилища в процентах от доступного объема диска.

  Информацию о доступном объеме диска вы можете получить из ClickHouse, отправив запрос:

  ```
  'SELECT hostname(), name, total_space FROM system.disks'
  ```

  Допустимые значения – от 1 до 95. Значение по умолчанию – 80. Если вы хотите использовать проценты для всех пространств хранилища, сумма процентов в условиях всех пространств не может превышать 95, но мы рекомендуем указывать ограничение не более 90% включительно для всего хранилища или для отдельных пространств.

  Не рекомендуется указывать значение меньше 5%, так как в этом случае возрастает вероятность потери данных в хранилище.

  > Если хранилище организовано в виде кластера из нескольких серверов, объем занятого дискового пространства определяется отдельно для каждого сервера. Данные для хранения могут распределяться между дисками на серверах неравномерно. В Kaspersky SIEM Cloud события будут перемещаться на диски холодного хранения или удаляться при достижении максимального размера хранилища *на одном из серверов в кластере*.

Механизм определения размера занятого пространства в хранилище

Определение размера занятого пространства в хранилище осуществляется следующим образом:

1. Информация о состоянии дисков и партиций Kaspersky SIEM Cloud получается со всех доступных реплик.

2. Если занятое пространство превышает установленные значения, Kaspersky SIEM Cloud осуществляет действия в зависимости от типа хранения данных: горячее или холодное.

   При горячем хранении данных для каждого доступного узла и пространства осуществляются следующие действия:

   a. Рассчитывается суммарный размер партиций этого пространства на реплике.

   b. Рассчитывается максимальный размер пространства на реплике:

   - Если установлено абсолютное значение для размера хранилища в ГБ, максимальный размер пространства на реплике рассчитывается следующим образом:

     `<maximum space size> = <configured threshold> / <number of replicas in the cluster>`

     Например, для кластера из трех шардов, в каждом из которых находятся две реплики, и установлено пороговое значение 6 ГБ, максимальный объем данных на реплике – 1 ГБ.

   - Если установлено относительное значение для размера хранилища в процентах, максимальный размер пространства на реплике рассчитывается следующим образом:

     `<maximum space size> = <space size on the replica> / <replica disk size> * 100%`

Размер диска реплики не включает в себя пространство, зарезервированное для `ext4`.

Если установленное пороговое значение превышено, партиции на хосте удаляются или переносятся в холодное хранилище. Партиции удаляются на всех шардах.

При холодном хранении данных для каждого доступного пространства партиции удаляются в соответствии с установленным значением времени хранения событий в Kaspersky SIEM Cloud (TTL).

Если вы хотите использовать дополнительное условие хранения, нажмите на кнопку **Добавить условие хранения** и укажите дополнительное условие хранения. Вы можете добавить не более двух условий и сочетать только условия следующих типов:

- дни и размер хранилища в ГБ;
- дни и размер хранилища в процентах.

Если вы хотите удалить условие хранения, нажмите на значок крестика возле этого условия.

7. В поле **Срок хранения событий аудита** укажите, в течение какого количества дней вы хотите хранить события аудита. Минимальное значение и значение по умолчанию: `365`.

8. Если вы хотите изменить параметры ClickHouse, в поле **Переопределение параметров ClickHouse** вставьте строки с параметрами из XML-файла конфигурации ClickHouse `/opt/kaspersky/kuma/clickhouse/cfg/config.xml`.

   Указание корневых элементов `<yandex>`, `</yandex>` не требуется. Переданные в поле параметры конфигурации будут использоваться вместо параметров по умолчанию.

   Пример

   ```
   <merge_tree>
   <parts_to_delay_insert>600</parts_to_delay_insert>
   <parts_to_throw_insert>1100</parts_to_throw_insert>
   </merge_tree>.
   ```

9. В блоке параметров **Узлы кластера ClickHouse** добавьте в хранилище узлы кластера ClickHouse.

   Узлов может быть несколько. Узлы можно добавить с помощью кнопки **Добавить узел** и удалить, нажав на значок крестика в блоке нужного узла.

   Укажите следующие параметры:

   - В поле **FQDN** укажите полное доменное имя добавляемого узла. Например, `kuma-storage-cluster1-server1.example.com`.
   - В полях **Идентификатор шарда**, **Идентификатор реплики** и **Идентификатор кипера** укажите роль узла в кластере ClickHouse.

     Идентификаторы шарда и кипера должны быть уникальными в рамках кластера. Идентификатор реплики должен быть уникальным в рамках шарда.

     Комбинация идентификаторов определяет положение узла в структуре кластера и его функциональное назначение:

     - Шард, реплика, кипер – узел участвует в накоплении и поиске нормализованных событий, а также в координации репликации данных на уровне всего кластера.
     - Шард, реплика – узел участвует в накоплении и поиске нормализованных событий.

- Кипер – узел не хранит нормализованные события, но участвует в координации репликации данных на уровне всего кластера.

  Выделенные узлы с ролью кипера рекомендуется указывать в начале списка в разделе **Мониторинг → Ресурсы и сервисы → Хранилища → <Хранилище> → Основные параметры → Узлы кластера ClickHouse**.

Ниже показан пример заполнения раздела **Узлы кластера ClickHouse** для хранилища с выделенными киперами в распределенной схеме установки. Вы можете адаптировать пример для своих потребностей.

Пример: узлы кластера ClickHouse

```
Полное доменное имя: kuma-storage-cluster1-server1.example.com
        Идентификатор шарда: 0
Идентификатор реплики: 0
Идентификатор кипера: 1
        Полное доменное имя: kuma-storage-cluster1server2.example.com
        Идентификатор шарда: 0
Идентификатор реплики: 0
Идентификатор кипера: 2
        Полное доменное имя: kuma-storage-cluster1server3.example.com
        Идентификатор шарда: 0
Идентификатор реплики: 0
Идентификатор кипера: 3
        Полное доменное имя: kuma-storage-cluster1server4.example.com
        Идентификатор шарда: 1
Идентификатор реплики: 1
Идентификатор кипера: 0
        Полное доменное имя: kuma-storage-cluster1server5.example.com
        Идентификатор шарда: 1
Идентификатор реплики: 2
Идентификатор кипера: 0
Полное доменное имя: kuma-storage-cluster1server6.example.com
        Идентификатор шарда: 2
Идентификатор реплики: 1
Идентификатор кипера: 0
        Полное доменное имя: kuma-storage-cluster1server7.example.com
        Идентификатор шарда: 2
Идентификатор реплики: 2
Идентификатор кипера: 0
```

10. Если вы хотите распределять хранимые объекты по пространствам, создайте их в блоке параметров **Пространства**.

    Как создать пространство в хранилище

    Пространств может быть несколько. Пространства можно добавить с помощью кнопки **Добавить пространство** и удалить, нажав на значок крестика в блоке нужного пространства.

    Укажите следующие параметры:

    1. В поле **Название** укажите название пространства: от 1 до 128 символов в кодировке Unicode.

    2. Если требуется, чтобы в пространство не поступали события, установите флажок **Только для чтения**.

       По умолчанию флажок снят.

    3. В поле **Варианты условий хранения** выберите для пространства условие хранения событий в кластере ClickHouse, при выполнении которого события будут переноситься на диски холодного хранения или удаляться, если холодное хранение не настроено или настроено неверно. В Kaspersky SIEM Cloud при добавлении пространства используется условие хранения **365 дней**.

Чтобы задать условие хранения для пространства, выполните одно из следующих действий:

- Если вы хотите ограничить срок хранения событий, в раскрывающемся списке выберите **Дни** и в поле укажите максимальный срок хранения событий в днях в кластере горячего хранилища ClickHouse.

  Минимальное значение – 1. Значение по умолчанию – 365.

- Если вы хотите ограничить максимальный размер пространства хранилища, в раскрывающемся списке выберите **ГБ** и в поле укажите максимальный размер пространства в гигабайтах.

  Минимальное значение и значение по умолчанию – 1.

- Если вы хотите ограничить размер пространства хранилища относительно объема диска, который доступен хранилищу, в раскрывающемся списке выберите **Проценты** и в поле укажите максимальный размер пространства в процентах от объема диска, доступного хранилищу. В этом случае условие также может сработать при уменьшении доступного хранилищу объема диска.

  Допустимые значения – от 1 до 95. Значение по умолчанию – 80. Если вы хотите использовать проценты для всех пространств хранилища, сумма процентов в условиях всех пространств не может превышать 95, но мы рекомендуем указывать ограничение не более 90% включительно для всего хранилища или для отдельных пространств.

  Не рекомендуется указывать малые значения процентов, так как в этом случае возрастает вероятность потери данных в хранилище.

  > При использовании размера в качестве условия хранения требуется следить, чтобы суммарный размер пространств, указанный в условиях хранения не превышал физический размер хранилища, иначе при запуске сервиса отобразится ошибка.

  > В условиях хранения с ограничением размера для всех пространствах хранилища используйте одинаковые единицы изменения (только в гигабайтах или только в процентах). Иначе, если для одного пространства условие задано в процентах, а для другого в гигабайтах, хранилище может переполниться из-за несоответствия значений и данные будут утеряны.

4. При необходимости в поле **Время хранения событий** укажите общую длительность хранения событий в Kaspersky SIEM Cloud с момента поступления, в днях. По истечении указанного срока события будут автоматически удалены с диска холодного хранения. Значение по умолчанию – 0.

   Параметр **Время хранения событий** становится доступен, только после того как вы добавили хотя бы один диск холодного хранения.

   Время хранения событий рассчитывается как сумма времени хранения событий в кластере горячего хранилища ClickHouse до наступления условия, заданного в параметре **Варианты условий хранения**, и времени хранения событий на диске холодного хранения. После наступления одного из условий хранения партиция данных за самую старую дату перемещается на диск холодного хранения и находится там до истечения времени хранения событий в Kaspersky SIEM Cloud.

   В зависимости от заданного условия хранения время хранения будет следующим:

   - Если вы задали условие хранения в днях и хотите, чтобы события попадали в холодное хранилище, значение параметра **Время хранения событий** должно быть больше количества дней, указанного в условии хранения. Срок холодного хранения событий будет рассчитан как **Время хранения событий** минус количество дней, указанное в параметре **Варианты условий хранения**.

     Если вы не хотите хранить события из этого пространства на диске холодного хранения, в параметре **Время хранения событий** вы можете указать такое же количество дней, как в условии хранения.

- Если вы задали условие хранения в гигабайтах или процентах и хотите, чтобы события попадали в холодное хранилище, рекомендуется указывать относительно большое значение параметра **Время хранения событий**, чтобы избежать удаления событий. Это связано с тем, что невозможно рассчитать точный срок, когда будут выполнены условия, указанные в параметре **Варианты условий хранения**.

  Если вы не хотите хранить события из этого пространства на диске холодного хранения, в параметре **Время хранения событий** вы можете указать значение 0.

5. Если вы хотите задать условия определения событий, которые будут перемещаться в пространство, в блоке параметров **Параметры фильтра** выберите готовый фильтр в раскрывающемся списке **Фильтр** или создайте новый, нажав кнопку **Создать**.

   Создание фильтра в ресурсах

   Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

   Чтобы создать фильтр:

   1. В раскрывающемся списке **Фильтр** выберите **Создать**.

   2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят.

   3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.

   4. Выберите режим создания фильтра: **Конструктор** или **Код**.

      При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра.

   5. Если вы выбрали вариант **Конструктор**, выполните следующие действия:

      a. В раскрывающемся списке выберите логический оператор:

         - **И** – отбирает события, которые соответствуют всем указанным условиям.
         - **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий.
         - **НЕ** – отбирает события, которые не соответствуют всем указанным условиям.

      b. Нажмите на кнопку **Добавить условие**.

      c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

      d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра.

Операнды фильтров

- **Поля событий** – поле события, которое требуется использовать как операнд фильтра.
- **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**.

  Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра.
- **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры:
  - **словарь** (обязательно) – словарь, который требуется использовать.
  - **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.
- **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события.
  - **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать.
  - **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы.
  - **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда.
  - **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда.
- **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
  - **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**.
  - **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.
- **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
  - **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
  - **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
  - **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.

- **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
  - **значение** (обязательно) – константа, которую требуется присвоить операнду.
- **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
  - **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.

Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в коррелляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.

Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.

e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.

Вы можете добавить несколько групп условий.

6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.

В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕.

8. Нажмите **Сохранить**.

После создания пространства можно просматривать и удалять в параметрах набора ресурсов хранилища.

Нет необходимости создавать отдельное пространство для событий аудита. События этого типа (Type=4) автоматически помещаются в отдельное пространство Audit со сроком хранения не менее 365 дней, которое недоступно для редактирования или удаления из веб-интерфейса Kaspersky SIEM Cloud.

11. Если вы хотите переносить события на длительное хранение из кластера ClickHouse на диски, добавьте диски в хранилище в блоке параметров **Диски холодного хранения**.

Как добавить диск в хранилище

Дисков может быть несколько. Диски можно добавить с помощью кнопки **Добавить диск** и удалить, нажав на значок крестика в блоке нужного диска.

Укажите следующие параметры:

1. В раскрывающемся списке **Тип** выберите тип доменного имени подключаемого диска **Локальный**.

2. В поле **Название** укажите название диска.

3. В поле **Путь** введите абсолютный путь директории смонтированного локального диска. Путь должен начинаться и оканчиваться символом "/".

   Владельцем директории смонтированного локального диска должен быть пользователь Kaspersky SIEM Cloud.

4. Вернитесь к блоку общих параметров и заполните следующие поля:

   - **Время хранения событий** – общая длительность хранения событий в Kaspersky SIEM Cloud с момента поступления, в днях. По истечении указанного срока события будут автоматически удалены с диска холодного хранения. Значение по умолчанию – 0.

     Время хранения событий рассчитывается как сумма времени хранения событий в кластере горячего хранилища ClickHouse до наступления условия, заданного в параметре **Варианты условий хранения**, и времени хранения событий на диске холодного хранения. После наступления одного из условий хранения партиция данных за самую старую дату перемещается на диск холодного хранения и находится там до истечения времени хранения событий в Kaspersky SIEM Cloud.

     В зависимости от заданного условия хранения время хранения будет следующим:

     - Если вы задали условие хранения в днях и хотите, чтобы события попадали в холодное хранилище, значение параметра **Время хранения событий** должно быть больше количества дней, указанного в условии хранения. Срок холодного хранения событий будет рассчитан как **Время хранения событий** минус количество дней, указанное в параметре **Варианты условий хранения**.

       Если вы не хотите хранить события из этого пространства на диске холодного хранения, в параметре **Время хранения событий** вы можете указать такое же количество дней, как в условии хранения.

     - Если вы задали условие хранения в гигабайтах или процентах и хотите, чтобы события попадали в холодное хранилище, рекомендуется указывать относительно большое значение параметра **Время хранения событий**, чтобы избежать удаления событий. Это связано с тем, что невозможно рассчитать точный срок, когда будут выполнены условия, указанные в параметре **Варианты условий хранения**.

       Если вы не хотите хранить события из этого пространства на диске холодного хранения, в параметре **Время хранения событий** вы можете указать значение 0.

   - **Срок холодного хранения событий аудита** – количество дней хранения событий аудита. Минимальное значение – 0.

12. При необходимости перейдите на вкладку **Дополнительные параметры** и задайте следующие параметры:

    - В поле **Размер буфера** укажите размер буфера в байтах, при достижении которого следует передать события в базу данных. Значение по умолчанию – 128 МБ. Если на виртуальной машине меньше свободной памяти, чем заданное значение **Размер буфера**, будет установлено ограничение в 128 МБ.

      Если ожидаемый трафик на сервис хранилища будет больше 1 Гбит/сек, рекомендуется изменить значение параметра **Размер буфера** в соответствии с известным вам значением и указать значение параметра **Интервал очистки буфера** равное 2.

Значение параметра **Размер буфера** можно определить опытным путем. Если на метрике хранилища **Insert QPS** показатель превышает 1 и видно, что накапливается очередь запросов, воспользуйтесь рекомендациями по расчету и корректировке значения параметра **Размер буфера**, приведенными в статье Просмотр метрик Kaspersky SIEM Cloud.

- В поле **Максимальный размер буфера** укажите максимальный размер буфера в байтах. Значение по умолчанию – 256 МБ.

  По умолчанию события записываются в базу данных раз в секунду. Если поток событий возрастает и события начинают записываться чаще, чем раз в секунду, размер буфера автоматически увеличивается. Буфер увеличится максимум в три раза от значения в поле **Размер буфера**, но не может превысить значения в поле **Максимальный размер буфера**. После увеличения размера буфера при нормализации нагрузки размер не меняется, автоматическое уменьшение буфера не предусмотрено.

  Если вы укажете значение в поле **Максимальный размер буфера** меньшим или равным значению в поле **Размер буфера**, то размер буфера не изменится.

  При перезапуске сервиса хранилища увеличенный размер буфера сбрасывается до значения в поле **Размер буфера**.

- В поле **Интервал очистки буфера** укажите интервал в секундах, в течение которого решение будет ждать заполнения буфера. Если буфер не заполнен и указанное время прошло, события передаются в базу данных. Значение по умолчанию – 1 с.

- В поле **Требуемый объем памяти** укажите минимальный размер свободной оперативной памяти в байтах. Значение по умолчанию – 0.

  Если на узле, на котором установлено хранилище, свободной оперативной памяти окажется меньше указанного значения, запрос на запись событий в базу данных вернет ошибку, события будут записаны позже. Ограничение размера памяти позволяет избежать ситуации, когда память переполняется, если по какой-либо причине запись событий в базу данных блокируется и данные начинают накапливаться в памяти.

- В поле **Ограничение размера дискового буфера** укажите значение в байтах.

  Дисковый буфер используется для временного размещения тех событий, которые не удалось отправить для дальнейшей обработки или хранения. Если выделенное под дисковый буфер дисковое пространство исчерпано, события ротируются по следующему правилу: новые события замещают самые старые события, записанные в буфер. Значение по умолчанию – 10 ГБ.

- С помощью переключателя **Дисковый буфер** включите или выключите использование дискового буфера. По умолчанию дисковый буфер включен.

- С помощью переключателя **Запись в локальную таблицу базы данных** включите или выключите запись в локальную таблицу базы данных. По умолчанию запись выключена.

  Если вы включите запись, она будет выполняться только на том узле, на котором установлено хранилище. Мы рекомендуем использовать эту функцию только при условии, что у вас настроена балансировка на коллекторе и/или коррелляторе: в коллекторе и/или коррелляторе на шаге **6. Маршрутизация** в разделе **Дополнительные настройки** в поле **Политика выбора URL** установлено значение **По очереди**.

  Если вы выключите запись, данные распределяются по шардам кластера.

Набор ресурсов для хранилища изменен.

После изменения параметров хранилища его сервис необходимо перезапустить.

Добавление пространства в хранилище

По умолчанию решение Kaspersky SIEM Cloud развертывается в типовой конфигурации, которая включает в себя сервис хранилища [OOTB] OSMP Storage. При необходимости вы можете увеличить объем доступного пространства в хранилище. Вы можете сделать это одним из следующих способов:

- Добавление пространства в имеющееся хранилище.
- Добавление шардов в имеющееся хранилище.

Добавлять пространство в хранилище любым из способов вы можете только при наличии у вас достаточного количества вычислительных единиц.

Добавление пространства в имеющееся хранилище

Чтобы добавить свободное пространство в хранилище:

1. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → Хранилища**.
2. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
3. Установите флажок рядом с ресурсом хранилища, к которому вы хотите добавить свободное пространство. Если хотите добавить пространство к предустановленному хранилищу, выберите **[OOTB] OSMP Storage**.
4. Нажмите на кнопку **Развернуть**.

   Откроется панель с параметрами выбранного сервиса.
5. Выберите шаблон сервиса и укажите новый размер хранилища.

   Kaspersky SIEM Cloud отображает количество вычислительных единиц, необходимых для установки сервиса в выбранной конфигурации. Если вам не хватает доступных вычислительных единиц, либо измените параметры сервиса, либо приобретите дополнительные вычислительные единицы.
6. Нажмите **Развернуть**.

Сервис хранилища разворачивается в облачной инфраструктуре в новой конфигурации.

Добавление шардов в имеющееся хранилище

Вы можете увеличить размер имеющегося хранилища, добавив к нему один или несколько шардов.

После добавления шардов в хранилище рекомендуется провести ребалансировку хранилища. В результате ребалансировки данные с заполненных шардов равномерно распределятся по всем шардам хранилища, включая добавленные пустые шарды.

Пример:

В вашем хранилище один шард размером 100 ГБ. Если вы добавите еще один пустой шард размером 100 ГБ, то после ребалансировки на каждом шарде будет приблизительно по 50 ГБ данных. Если вы добавите не один, а два шарда по 100 ГБ, то после ребалансировки на каждом шарде будет приблизительно по 33 ГБ данных.

Ребалансировку может выполнять только пользователь с ролью Главный администратор.

Чтобы добавить свободное пространство в хранилище:

1. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → Хранилища**.
2. Установите флажок рядом с ресурсом хранилища, к которому вы хотите добавить свободное пространство. Если хотите добавить пространство к предустановленному хранилищу, выберите **[ООТВ] OSMP Storage**.
3. В блоке параметров **Узлы кластера ClickHouse** добавьте в хранилище узлы кластера ClickHouse.

   Узлов может быть несколько. Узлы можно добавить с помощью кнопки **Добавить узел** и удалить, нажав на значок крестика в блоке нужного узла.

   Укажите следующие параметры:

   - В поле **FQDN** укажите полное доменное имя добавляемого узла. Например, `kuma-storage-cluster1-server1.example.com`.
   - В полях **Идентификатор шарда**, **Идентификатор реплики** и **Идентификатор кипера** укажите роль узла в кластере ClickHouse.

     Идентификаторы шарда и кипера должны быть уникальными в рамках кластера. Идентификатор реплики должен быть уникальным в рамках шарда.

     Комбинация идентификаторов определяет положение узла в структуре кластера и его функциональное назначение:

     - Шард, реплика, кипер – узел участвует в накоплении и поиске нормализованных событий, а также в координации репликации данных на уровне всего кластера.
     - Шард, реплика – узел участвует в накоплении и поиске нормализованных событий.
     - Кипер – узел не хранит нормализованные события, но участвует в координации репликации данных на уровне всего кластера.

       Выделенные узлы с ролью кипера рекомендуется указывать в начале списка в разделе **Мониторинг → Ресурсы и сервисы → Хранилища → <Хранилище> → Основные настройки → Узлы кластера ClickHouse**.
4. Сохраните изменения.
5. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
6. Нажмите на кнопку **Добавить**, затем выберите **Добавить сервис**.

   Откроется окно **Выберите сервис**.
7. Установите флажок рядом с измененным хранилищем, затем нажмите **Создать сервис**.

   Сервис добавляется в список активных сервисов.

8. Установите флажок рядом с измененным хранилищем и нажмите на кнопку **Развернуть**.

   Откроется панель с параметрами выбранного сервиса.

9. Выберите шаблон сервиса и укажите другие параметры. Рекомендуется создавать шарды такого же размера, как и уже имеющиеся в хранилище.

   Kaspersky SIEM Cloud отображает количество вычислительных единиц, необходимых для установки сервиса в выбранной конфигурации. Если вам не хватает доступных вычислительных единиц, либо измените параметры сервиса, либо приобретите дополнительные вычислительные единицы.

10. Нажмите **Развернуть**.

Сервис создан и установлен в облачной инфраструктуре.

Ребалансировка хранилища

В результате ребалансировки Kaspersky SIEM Cloud переносит партиции из более заполненных шардов-источников в менее заполненные или пустые целевые шарды. Анализ и перенос партиций происходит по дням. Перед переносом партиций за определенный день Kaspersky SIEM Cloud оценивает размер партиций и свободное место в целевом шарде. Если места достаточно, данные переносятся. Если места недостаточно, то есть потенциальный перенос данных приведет к неравномерному распределению данных по шардам, перенос не происходит и ребалансировка останавливается.

Kaspersky SIEM Cloud не переносит:

- Данные из холодного хранилища и хранилища S3.
- Партиции за последние два дня (день запуска ребалансировки и предыдущий день). Kaspersky SIEM Cloud анализирует и переносит только более ранние партиции.

Чтобы выполнить ребалансировку хранилища после добавления шардов:

1. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
2. Установите флажок рядом с хранилищем, которое вы хотите ребалансировать.
3. В меню (⋮) выберите **Перейти к шардам**.

   Откроется окно **Шарды**.

4. Выберите добавленные пустые шарды и нажмите на кнопку **Ребалансировать**. Данные будут перенесены с заполненных шардов на выбранные вами шарды.

Выполняется ребалансировка хранилища. За процессом ребалансировки вы можете следить по статусам шардов в окне **Шарды**. Если вы остановите процесс ребалансировки, Kaspersky SIEM Cloud завершит перенос партиций, которые на момент остановки оказались частично перенесены, и затем остановит ребалансировку.

Для отслеживания процесса ребалансировки Kaspersky SIEM Cloud создает следующие события аудита:

- Ребалансировка запущена.
- Ребалансировка остановлена.

- Ребалансировка успешно завершена.
- Ошибка при выполнении ребалансировки.

Просмотр разделов хранилища

Создав и установив сервис хранилища, вы можете просмотреть его разделы, а также при необходимости удалить.

Просмотр разделов хранилища

Чтобы просмотреть разделы хранилища:

1. В веб-интерфейсе откройте раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
2. Установите флажок рядом с хранилищем, разделы которого вы хотите просмотреть.
3. В панели инструментов или в меню (⋮) нажмите **Смотреть разделы**.

   Откроется таблица разделов хранилища. При просмотре вы можете переключаться между вкладками **Горячее хранилище** и **Холодное хранилище**.

Таблицу можно сортировать по тенанту, дате создания раздела, названию и размеру раздела, началу холодного хранения и окончанию хранения данных, нажав на значок сортировки ⌄ в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

Таблица содержит следующие столбцы:

- **Тенант** – название тенанта, которому принадлежат хранимые данные. Вы можете отфильтровать таблицу по конкретным тенантам. Для этого нажмите на заголовок столбца и установите флажки рядом с нужными тенантами.
- **Создан** – дата создания раздела.
- **Пространство** – название раздела. Вы можете отфильтровать таблицу по конкретным разделам. Для этого нажмите на заголовок столбца и установите флажки рядом с нужными разделами.
- **Размер** – размер раздела. Нажав на заголовок столбца, вы можете выбрать, отображать данные в байтах, мегабайтах, гигабайтах или терабайтах.
- **События** – количество хранимых событий.
- **Начало холодного хранения** – дата, когда данные будут перенесены с кластеров ClickHouse на диски для холодного хранения.
- **Окончание хранения** – дата, когда истекает срок действия раздела. По достижении этого срока раздел и содержащиеся в нем события перестают быть доступны.

Удаление разделов хранилища

Невозможно удалить разделы для событий аудита.

Чтобы удалить раздел:

1. В веб-интерфейсе откройте раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
2. Установите флажок рядом с хранилищем, разделы которого вы хотите просмотреть.
3. В панели инструментов или в меню (⋮) нажмите **Смотреть разделы**.
4. В таблице разделов хранилища установите флажок рядом с нужным разделом и нажмите **Удалить**.

   Откроется окно подтверждения.
5. Нажмите **OK**.

Раздел будет удален.

Просмотр активных запросов в ClickHouse

Вы можете просматривать и отменять запросы других пользователей и ресурсов Kaspersky SIEM Cloud, которые выполняются в текущий момент.

Для просмотра и отмены запросов требуется учетная запись с правами Главного администратора

Просмотр активных запросов

Чтобы просмотреть таблицу активных запросов:

1. В веб-интерфейсе откройте раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
2. Установите флажки рядом с нужными хранилищами.
3. В панели инструментов или в меню (⋮) нажмите **Активные запросы**.

   Откроется таблица активных запросов в ClickHouse. Если вы выбрали несколько хранилищ, в таблице отобразятся активные запросы из каждого выбранного хранилища.

Таблицу можно сортировать, нажав на значок сортировки ⌄ в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

Таблица содержит следующие столбцы:

- **Запущен** – дата и время, когда был запущен запрос.
- **Создал** – инициатор запроса. Для пользовательских запросов отображается имя пользователя Kaspersky SIEM Cloud. Для запросов типа **Ресурс** отображается название ресурса.
- **Запрос** – текст SQL-запроса, выполняемого в ClickHouse.
- **Тип** – тип запроса:
  - **В фоне** – пользовательский запрос, запущенный в фоновом режиме по кнопке **Запустить в фоне**.
  - **Ресурс** – служебный SQL-запрос, инициированный ресурсом Kaspersky SIEM Cloud в процессе работы, например при обработке или анализе данных.
  - **Пользовательский** – SQL-запрос, запущенный пользователем по кнопке **Выполнить запрос** и выполняемый в обычном режиме.
- **Хранилище** – название хранилища ClickHouse, в котором выполняется запрос.

При необходимости вы можете настроить отображение столбцов в таблице, нажав на значок шестеренки . Для обновления данных нажмите на значок обновления .

Отмена запросов

Чтобы отменить выполняющиеся запросы:

1. В веб-интерфейсе откройте раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
2. Установите флажки рядом с нужными хранилищами.
3. В панели инструментов или в меню (⋮) нажмите **Активные запросы**.
4. В таблице установите флажки рядом с одним или несколькими запросами, которые вы хотите отменить, и нажмите **Отменить запросы**.

   Откроется окно подтверждения.
5. При необходимости в поле **Укажите причину** укажите причину отмены запросов.
6. Нажмите **OK**.

Запросы будут отменены и удалены из таблицы. Автоматически создастся событие аудита.

Холодное хранение событий

В Kaspersky SIEM Cloud можно настроить перенос устаревших данных с кластера ClickHouse в холодное хранилище. Для холодного хранения могут использоваться смонтированные в операционной системе локальные диски, распределенная файловая система Hadoop Distributed File System (HDFS) или облачное хранилище S3 (англ. Simple Storage Service).

Не рекомендуется использовать HDFS в качестве холодного хранилища. Поддержка файловой системы HDFS будет прекращена в одном из будущих релизов. Пользователям, работающим с HDFS, рекомендуется запланировать переход на использование S3.

Функция холодного хранения включается, если при создании хранилища был указан хотя бы один диск холодного хранения. Если используется несколько хранилищ, на каждом узле с данными должен быть смонтирован диск холодного хранения или диск HDFS или S3 по пути, указанному в конфигурации хранилища.

Работа сервиса хранилища может нарушаться и его последующий запуск становится невозможным в следующих случаях:

- Диск холодного хранения не настроен, и на сервере в горячем хранилище закончилось место.
- Диск холодного хранения настроен, и на нем закончилось место.
- Кластер не может получить доступ к настроенному диску холодного хранения.

Для того чтобы избегать таких ситуаций, мы рекомендуем добавлять пользовательские условия хранения событий в горячем хранилище.

Вы можете добавить диски холодного хранения при создании набора ресурсов для хранилища, а также удалить их. Если вы добавили несколько дисков холодного хранения, данные будут записываться на них по принципу чередования (англ. round-robin) по круговому циклу. Если данные, которые необходимо записать на диск, занимают больше места, чем свободно на этом диске, эти данные и все последующие будут записываться по принципу чередования на следующие диски холодного хранения. Если вы добавили только два диска холодного хранения, данные будут записываться на тот диск, на котором есть свободное место.

После изменения параметров холодного хранения сервис хранилища необходимо перезапустить. Если сервис не запускается, причина будет указана в журнале хранилища.
Сервис хранилища также необходимо перезапустить, если путь к хранилищу S3 был указан неправильно. При этом созданный файл `storage.xml` автоматически не удаляется. Вам нужно вручную очистить папку `/opt/kaspersky/kuma/clickhouse/cfg/config.d/` и заново настроить параметры холодного хранилища.

Если указанный в параметрах хранилища диск холодного хранения стал недоступен (например, вышел из строя), это может привести к ошибкам в работе сервиса хранилища. В этом случае необходимо воссоздать диск с таким же путем (для локальных дисков) или таким же адресом (для дисков HDFS и S3), а затем удалить его из параметров хранилища.

Правила переноса данных на диски холодного хранения

Вы можете настроить условия хранения событий в горячем хранилище кластера ClickHouse, задав ограничение по сроку хранения или по максимальному размеру хранилища. При задействованном холодном хранении Kaspersky SIEM Cloud раз в 15 минут и после перезагрузки Ядра Kaspersky SIEM Cloud проверяет выполнение заданных условий хранения следующим образом:

1. Kaspersky SIEM Cloud получает партиции для проверяемого хранилища и группирует их по дискам холодного хранения и пространствам.

2. Для каждого пространства Kaspersky SIEM Cloud проверяет, выполняется ли заданное условие хранения.

3. Если условие выполняется (например, в пространстве есть события, хранящиеся дольше указанного срока, или размер хранилища достиг или превышает указанное в условии значение), Kaspersky SIEM Cloud переносит все партиции за самую старую дату на диски холодного хранения либо удаляет эти партиции, если диск холодного хранения не настроен или настроен неверно. Это действие повторяется до тех пор, пока в пространстве выполняется заданное условие хранения, например, если после удаления партиций за одну дату размер хранилища все еще превышает заданный в условии максимальный размер.

   При начале и окончании переноса или удалении данных Kaspersky SIEM Cloud создает события аудита.

   Перенос и обработка событий выполняются на уровне партиций. Подробнее об управлении партициями см. раздел Отключение, архивирование и подключение партиций.

4. Если настроен срок хранения данных в Kaspersky SIEM Cloud, при переносе партиций на диски холодного хранения проверяется, выполняются ли на диске заданные условия. Если на диске обнаружены события, хранящиеся дольше срока, заданного в параметре **Время хранения событий**, который рассчитывается с момента поступления событий в Kaspersky SIEM Cloud, решение удаляет эти события или все партиции за самую старую дату.

   При удалении данных Kaspersky SIEM Cloud создает события аудита.

> Если диски кластера ClickHouse заполнены на 97%, самые большие партиции либо автоматически переносятся на диски холодного хранения, либо удаляются, если дисков холодного хранения нет.

Во время переноса данных сервис хранилища продолжает работать, при этом в разделе **Ресурсы** → **Активные сервисы** для него сохраняется зеленый статус. При наведении курсора мыши на значок статуса отображается сообщение о переносе данных. При удалении холодного диска сервис хранилища отображается в желтом статусе.

Особенности хранения событий и доступа к ним

- При использовании HDFS-дисков для холодного хранения требуется обеспечить защиту данных одним из следующих способов:

  - Настроить отдельный физический интерфейс в сети VLAN, в котором будут расположены только HDFS-диски и кластер ClickHouse.

  - Настроить правила сегментации сети и фильтрации трафика, исключающие прямой доступ к HDFS-диску или перехват трафика к диску со стороны ClickHouse.

- События, находящиеся в кластере ClickHouse и на дисках холодного хранения, одинаково доступны в веб-интерфейсе Kaspersky SIEM Cloud, например, при поиске событий или при просмотре событий, относящихся к алертам.

- Допускается не хранить события или события аудита на дисках холодного хранения. Для этого в параметрах хранилища нужно выполнить следующие действия:

  - Если вы не хотите хранить события на дисках холодного хранения, выполните одно из следующих действий:

    - Если в поле **Варианты условий хранения** выбрано условие хранения в гигабайтах или процентах, в поле **Время хранения событий** укажите значение `0`.

    - Если в поле **Варианты условий хранения** выбрано условие хранения в днях, в поле **Время хранения событий** укажите такое же значение дней, как в поле **Варианты условий хранения**.

  - Если вы не хотите хранить события аудита на дисках холодного хранения, в поле **Срок холодного хранения событий аудита** укажите значение `0` (дней).

Особенности использования HDFS-дисков

- Перед подключением HDFS-дисков на них требуется создать директории для каждого узла кластера ClickHouse в формате `<хост HDFS-диска>/<идентификатор шарда>/<идентификатор реплики>`. Например, если кластер состоит из двух узлов, на которых расположены две реплики одного шарда, нужно создать следующие директории:

  - `hdfs://hdfs-example-1:9000/clickhouse/1/1/`

  - `hdfs://hdfs-example-1:9000/clickhouse/1/2/`

  События из узлов кластера ClickHouse будут переноситься в директории, в названии которых указаны идентификаторы их шарда и реплики. Если изменить эти параметры узла и при этом не создать соответствующую директорию на HDFS-диске, события при переносе могут быть потеряны.

- HDFS-диски, добавленные к хранилищу, работают в режиме JBOD. Это означает, что при отказе одного из дисков будет потерян доступ к хранилищу. При использовании HDFS следует учитывать необходимость отказоустойчивости и настроить RAID, а также хранение данных из разных реплик на различных устройствах.

- Скорость записи событий в HDFS, как правило, ниже скорости записи событий на локальные диски. Скорость доступа к событиям в HDFS, как правило, значительно ниже скорости доступа к событиям на локальных дисках. При использовании одновременно локальных дисков и HDFS-дисков запись будет происходить в них по очереди.

- HDFS используется только в качестве распределенного хранилища файловых данных ClickHouse. Для сжатия данных используются механизмы сжатия ClickHouse, а не HDFS.

- Сервер ClickHouse должен иметь доступ к соответствующему хранилищу HDFS с правами на запись.

Удаление дисков холодного хранения

Перед физическим отключением дисков холодного хранения необходимо удалить эти диски из параметров хранилища.

Чтобы удалить диск из параметров хранилища:

1. В веб-интерфейсе перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Хранилища** и выберите нужное хранилище.

2. В открывшемся окне в блоке параметров **Диски холодного хранения** в блоке параметров нужного диска нажмите на значок крестика, чтобы удалить диск.

3. В окне подтверждения нажмите **OK**.

   Данные с удаляемого диска автоматически начинают переноситься на другие диски холодного хранения или, если их нет, в кластер ClickHouse. В процессе переноса данных значок статуса хранилища подсвечивается желтым цветом и отображается значок песочных часов. При запуске и окончании переноса данных создаются события аудита.

   По завершении переноса событий диск автоматически удаляется из параметров хранилища. Теперь его можно безопасно отключить.

На удаляемых дисках могут оставаться события. Если вы хотите их удалить, вы можете, например, вручную удалить партиции с данными с помощью команды:

```
ROP PARTITION
```

Если указанный в параметрах хранилища диск холодного хранения стал недоступен (например, вышел из строя), это может привести к ошибкам в работе сервиса хранилища. В этом случае необходимо создать диск с таким же путем (для локальных дисков) или таким же адресом (для HDFS и S3-дисков), а затем удалить его из параметров хранилища.

Отключение, архивирование и подключение партиций

Если вы хотите оптимизировать дисковое пространство и ускорить выполнение запросов в Kaspersky SIEM Cloud, вы можете отключить в ClickHouse партиции с данными, архивировать партиции или перенести их на носитель. При необходимости вы можете снова подключить необходимые партиции и выполнить обработку данных.

Вы также можете использовать созданные архивы с партициями в качестве резервных копий этих партиций.

Отключение партиций

Чтобы отключить партиции:

1. Выберите шард, на всех репликах которого вы планируете отключить партицию.

2. Получите идентификатор партиции с помощью следующей команды:

   ```
   sudo /opt/kaspersky/kuma/storage/<repository ID>/deps/clickhouse/bin/client.sh -d kuma --multiline --query
   "SELECT partition, name FROM system.parts;" |grep 20231130
   ```

   В приведенном примере в результате выполнения команды будет получен идентификатор партиции от 30 ноября 2023 года.

3. На каждой реплике шарда отключите партицию с помощью следующей команды, указав полученный идентификатор:

   ```
   sudo /opt/kaspersky/kuma/storage/<repository ID>/deps/clickhouse/bin/client.sh -d kuma --multiline --query
   "ALTER TABLE events_local_v2 DETACH PARTITION ID '<partition ID>'"
   ```

Партиция отключена на всех репликах шарда. Теперь вы можете перенести данные на носитель или заархивировать партицию.

Архивирование партиций

Чтобы архивировать отключенные партиции:

1. Найдите отключенную партицию в дисковой подсистеме сервера:

   ```
   sudo find /opt/kaspersky/kuma/clickhouse/data/ -name <disabled partition ID>\*
   ```

2. Перейдите в директорию `detached` с отключенной партицией и выполните архивирование:

   ```
   sudo cd <path to the detached directory containing the disabled partition>
   sudo zip -9 -r detached.zip *
   ```

   Пример

   ```
   sudo cd /opt/kaspersky/kuma/clickhouse/data/store/d5b/d5bdd8d8-e1eb-4968-95bd-d8d8e1eb3968/detached/
   sudo zip -9 -r detached.zip *
   ```

Архивирование партиции выполнено.

Подключение партиций

Чтобы подключить архивные партиции к решению:

1. В веб-интерфейсе откройте раздел **Мониторинг** → **Ресурсы и сервисы** → **Хранилище** и в параметрах используемого хранилища увеличьте значение параметра **Время хранения событий**.

   Данные удаляются в соответствии с датой, указанной в поле Timestamp (когда событие получено), и в соответствии со значением параметра **Время хранения событий**, которое вы задали для хранилища.

   Перед тем как выполнять восстановление архивных данных, убедитесь, что значение параметра **Время хранения событий** больше даты, указанной в поле Timestamp. В противном случае, архивные данные будут удалены в течение 1 часа.

2. Поместите архивную партицию в директорию `detached` вашего хранилища и распакуйте архив:

   ```
   sudo unzip detached.zip -d <path to the detached directory>
   ```

   Пример

   ```
   sudo unzip detached.zip -d /opt/kaspersky/kuma/clickhouse/data/store/d5b/d5bdd8d8-e1eb-4968-95bd-d8d8e1eb3968/detached/
   ```

3. Подключите партицию с помощью команды:

   ```
   sudo /opt/kaspersky/kuma/storage/<repository ID>/deps/clickhouse/bin/client.sh -d kuma --multiline --query "ALTER TABLE events_local_v2 ATTACH PARTITION ID '<partition ID>'"
   ```

4. Повторите шаги распаковки архива и подключения партиции на каждой реплике шарда.

Архивная партиция подключена, и события снова доступны для поиска.

Резервное копирование партиций по расписанию

Настроить резервное копирование партиций по расписанию могут только пользователи с ролью Главный администратор.

Вы можете настроить и использовать резервное копирование партиций и холодное хранение событий одновременно. Резервная копия позволяет восстановить партиции при необходимости.

Чтобы настроить резервное копирование по расписанию:

1. В веб-интерфейсе откройте раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**.

   В открывшейся таблице при необходимости в столбце **Тип** выберите **Хранилище**.

2. Откройте действующее хранилище для настройки параметров. Для этого в столбце **Сервис** нажмите на название хранилища.

3. В открывшемся окне **Редактирование хранилища** на вкладке **Основные параметры** в блоке **Настройка резервного копирования и восстановления** настройте следующие параметры:

   a. В поле **Резервное копирование хранилища** укажите путь хранения файла резервной копии, например `/mnt/data`.

      Требования к пути:

      - Путь должен существовать и быть одинаковым на всех узлах кластера хранения.
      - У пользователя должны быть права на чтение, запись и исполнение файлов в указанной директории.
      - Указанная директория должна быть второго или более глубокого уровня вложенности. Не допускается использовать директорию первого уровня вложенности, например `/backup`.
      - Имя директории не должно содержать точку.
      - **Путь не должен содержать перечисленные префиксы**.

        Префиксы, которые невозможно использовать при указании путей к файлам:

        - `/*`
        - `/bin`
        - `/boot`
        - `/dev`
        - `/etc`
        - `/home`
        - `/lib`
        - `/lib64`
        - `/proc`
        - `/root`
        - `/run`
        - `/sys`
        - `/tmp`
        - `/usr/*`
        - `/usr/bin/`
        - `/usr/local/*`
        - `/usr/local/sbin/`
        - `/usr/local/bin/`

- `/usr/sbin/`
- `/usr/lib/`
- `/usr/lib64/`
- `/var/*`
- `/var/lib/`
- `/var/run/`
- `/opt/kaspersky/kuma/`

Приведенные префиксы используются системой в качестве регулярных выражений для проверки пути. Символ * в префиксах соответствует любой последовательности символов и не должен указываться в самом пути вручную, если это не часть допустимого пути.

Файлы по указанным ниже путям доступны:

- `/opt/kaspersky/kuma/clickhouse/logs/`
- `/opt/kaspersky/kuma/metrics/log/`

Убедитесь, что у пользователя есть права доступа к указанной директории. Если путь хранения не будет указан, выполнить резервное копирование будет невозможно.

b. Включите переключатель **Добавить автоматическое копирование**.

c. В поле **Резервное копирование через несколько дней** укажите целое число, которое означает, через сколько дней после создания партиции следует выполнять резервное копирование. Например, при значении **1** резервное копирование будет выполняться для партиции, созданной позавчера.

d. В раскрывающемся списке **Реплики** выберите одну реплику, для которой следует выполнить резервное копирование. При выборе нескольких реплик одного шарда произойдет дублирование данных.

Если в кластере используется несколько шардов, список **Реплики** будет содержать только те реплики, идентификаторы которых указаны во всех шардах.

4. В блоке **Партиции** нажмите **Добавить партицию** и настройте следующие параметры:

a. В раскрывающемся списке **Тенант** выберите тенант, в котором находится партиция для резервного копирования.

b. В раскрывающемся списке **Пространства** выберите одно или несколько пространств хранилища, которые принадлежат партиции для резервного копирования. Если значение не указано, будет выполнено резервное копирование партиции целиком.

Вы можете настроить параметры для нескольких партиций. Для этого нажмите **Добавить партицию** и настройте параметры в отобразившихся полях. Например, если вы хотите выполнить резервное копирование пространства **Audit** и у вас 10 тенантов, необходимо настроить резервное копирование отдельно для каждого тенанта.

5. Нажмите **Сохранить**.

   После сохранения параметров по указанному пути будут автоматически созданы директории `backup` и `restore`. В директории `backup` будут автоматически созданы вложенные директории с идентификатором тенанта и идентификатором пространства. Например, если вы указали путь хранения резервной копии `/mnt/data`, полный путь к файлу резервной копии будет выглядеть следующим образом: `/mnt/data/backup/<идентификатор тенанта>/<идентификатор пространства хранилища>/<дата создания партиции>.zip`. Узнать идентификатор тенанта или пространства можно в разделе **События** на карточке события.

Резервное копирование партиций по расписанию будет настроено. После запуска резервного копирования партиций создаются соответствующая задача и событие аудита. В случае неуспешного выполнения резервного копирования сервису хранилища в разделе **Активные сервисы** будет присвоен желтый статус и при наведении курсора мыши на желтый статус отобразится сообщение об ошибке. При очередном запуске резервного копирования по расписанию сначала происходит попытка резервного копирования старых данных.

Резервное копирование партиций вручную

Настроить резервное копирование партиций по расписанию могут только пользователи с ролью Главный администратор.

Вы можете настроить и использовать резервное копирование партиций и холодное хранение событий одновременно. Резервная копия позволяет восстановить партиции при необходимости.

Чтобы создать резервную копию партиции вручную:

1. В веб-интерфейсе откройте раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**.

   В открывшейся таблице при необходимости в столбце **Тип** выберите **Хранилище**.

2. Откройте действующее хранилище для настройки параметров. Для этого в столбце **Сервис** нажмите на название хранилища.

3. В открывшемся окне **Редактирование хранилища** перейдите на вкладку **Основные параметры**.

4. В блоке **Настройка резервного копирования и восстановления** в поле **Резервное копирование хранилища** укажите путь хранения файла резервной копии, например `/mnt/data`.

   Требования к пути:

   - Путь должен существовать и быть одинаковым на всех узлах кластера хранения.
   - У пользователя должны быть права на чтение, запись и исполнение файлов в указанной директории.
   - Указанная директория должна быть второго или более глубокого уровня вложенности. Не допускается использовать директорию первого уровня вложенности, например `/backup`.
   - Имя директории не должно содержать точку.

- **Путь не должен содержать перечисленные префиксы**.

  Префиксы, которые невозможно использовать при указании путей к файлам:

  - `/*`
  - `/bin`
  - `/boot`
  - `/dev`
  - `/etc`
  - `/home`
  - `/lib`
  - `/lib64`
  - `/proc`
  - `/root`
  - `/run`
  - `/sys`
  - `/tmp`
  - `/usr/*`
  - `/usr/bin/`
  - `/usr/local/*`
  - `/usr/local/sbin/`
  - `/usr/local/bin/`
  - `/usr/sbin/`
  - `/usr/lib/`
  - `/usr/lib64/`
  - `/var/*`
  - `/var/lib/`
  - `/var/run/`
  - `/opt/kaspersky/kuma/`

Приведенные префиксы используются системой в качестве регулярных выражений для проверки пути. Символ * в префиксах соответствует любой последовательности символов и не должен указываться в самом пути вручную, если это не часть допустимого пути.

Файлы по указанным ниже путям доступны:

- `/opt/kaspersky/kuma/clickhouse/logs/`
- `/opt/kaspersky/kuma/metrics/log/`

5. Сохраните внесенные изменения.
6. В разделе **Ресурсы** → **Активные сервисы** установите флажок рядом с сервисом хранилища в зеленом статусе.
7. В панели инструментов или в меню (⋮) выберите **Резервное копирование** и нажмите **Создать резервную копию**.

   Параметр **Создать резервную копию** доступен, если выбран один сервис хранилища в зеленом статусе.

   Параметр недоступен в следующих случаях:

   - Вы установили флажки рядом с несколькими сервисами.
   - Сервис хранилища находится в красном статусе.
   - Не установлен ни один флажок.
   - Вы установили флажок рядом с другим типом сервиса.
8. В открывшемся окне **Резервное копирование партиций** настройте следующие параметры:
   a. В раскрывающемся списке **Тенант** выберите тенант, в котором находится партиция для резервного копирования.
   b. В раскрывающемся списке **Пространства** выберите одно или несколько пространств хранилища, которые принадлежат партиции для резервного копирования. Если значение не указано, будет выполнено резервное копирование партиции целиком.
   c. В раскрывающемся списке **Реплики** выберите одну или все реплики, для которых следует выполнить резервное копирование. При выборе нескольких реплик одного шарда произойдет дублирование данных.
   d. В поле **Диапазон дат** укажите с помощью календаря диапазон дат для партиций, которые войдут в резервную копию.
9. Нажмите **OK**.
10. В окне подтверждения нажмите **OK**.

    После сохранения параметров по указанному пути будут автоматически созданы директории `backup` и `restore`. В директории `backup` будут автоматически созданы вложенные директории с идентификатором тенанта и идентификатором пространства. Например, если вы указали путь хранения резервной копии `/mnt/data`, полный путь к файлу резервной копии будет выглядеть следующим образом: `/mnt/data/backup/<идентификатор тенанта>/<идентификатор пространства хранилища>/<дата создания партиции>.zip`. Если вам необходимо узнать идентификатор тенанта или пространства, вы перейдите в раздел **События**, откройте карточку события и просмотрите информацию.

Если имя файла при резервном копировании вручную совпало с именем файла резервной копии по расписанию, возвращается ошибка о невозможности сохранить файл резервной копии. Нужно переименовать или удалить файл и выполнить резервное копирование вручную еще раз.

Резервное копирование партиций вручную будет выполнено. После запуска резервного копирования партиций создаются соответствующая задача и событие аудита. В случае неуспешного выполнения резервного копирования сервису хранилища в разделе **Активные сервисы** будет присвоен желтый статус и при наведении курсора мыши на желтый статус отобразится сообщение об ошибке.

Восстановление партиций из резервной копии

Восстановление партиций из резервной копии доступно только пользователям с ролью Главный администратор.

Чтобы выполнить восстановление партиции из резервной копии:

1. Перенесите ZIP-файл резервной копии из директории `backup` в директорию `restore`.
2. Предоставьте пользователю Kaspersky SIEM Cloud права доступа к ZIP-файлу резервной копии в директории `restore` с помощью следующей команды:

   ```
   sudo chown kuma *.zip
   ```

3. В веб-интерфейсе решения в разделе **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы** установите флажок рядом с сервисом хранилища в зеленом статусе.
4. В панели инструментов или в меню (⋮) выберите **Резервное копирование** → **Восстановить**.
5. В открывшемся окне **Восстановление из текущей установки KUMA** в раскрывающемся списке **Реплики** выберите одну реплику, в которой будет выполнено восстановление из резервной копии.
6. Нажмите **OK**.
7. В открывшемся окне подтверждения нажмите **OK**.

Партиции будут восстановлены из резервной копии. Также будут созданы соответствующая задача и событие аудита.

Импорт партиций из стороннего экземпляра Kaspersky SIEM Cloud

Импорт партиций из стороннего экземпляра Kaspersky SIEM Cloud доступен пользователям с ролью Главный администратор.

Чтобы импортировать партиции из стороннего экземпляра Kaspersky SIEM Cloud:

1. Поместите ZIP-файл для импорта партиций в директорию `restore`. Из этой директории будет выполняться импорт партиций.

2. Предоставьте пользователю Kaspersky SIEM Cloud права доступа к zip-файлу резервной копии в директории `restore` с помощью следующей команды:

   ```
   sudo chown kuma *.zip
   ```

3. В веб-интерфейсе решения в разделе **Мониторинг → Ресурсы и сервисы → Активные сервисы** установите флажок рядом с сервисом хранилища в зеленом статусе.

4. В панели инструментов или в меню (⋮) выберите **Резервное копирование → Импортировать**.

5. В открывшемся окне **Импорт из сторонней установки KUMA** выполните следующие действия:

   a. В раскрывающемся списке **Тенант** выберите тенант, для которого будет выполняться импорт партиций.

   b. В раскрывающемся списке **Реплики** выберите одну реплику, в которую будут импортированы партиции.

   c. В раскрывающемся списке **Поля для исключений** установите флажки рядом с полями, которые нужно удалить при импорте.

      По умолчанию установлены флажки для следующих полей:

      - AggregationRuleName.
      - CorrelationRuleName.
      - SourceAccountID.
      - DestinationAccountID.
      - SourceAssetID.
      - DestinationAssetID.
      - DeviceAssetID.
      - Поля расширенной схемы событий Kaspersky SIEM Cloud:
        - Поля расширенной схемы событий (SA., F., N. и прочие).
        - Поля активов KSC.
        - KLCorrelationRulePriority = "KL_CorrelationRulePriority"
        - KLSourceAssetDisplayName = "KL_SourceAssetDisplayName"
        - KLDestinationAssetDisplayName = "KL_DestinationAssetDisplayName"
        - KLDeviceAssetDisplayName = "KL_DeviceAssetDisplayName"

- KLSourceAccountDisplayName = "KL_SourceAccountDisplayName"
- KLDestinationAccountDisplayName = "KL_DestinationAccountDisplayName"
- KLDllHijackingResult = "KL_AI_DLLHijackingCheckResult"

При выборе группы **Поля расширенной схемы событий KUMA** выполняется удаление всей группы полей. Невозможно удалить только часть полей.

По умолчанию следующие поля будут удалены и поэтому недоступны для выбора в веб-интерфейсе:

- ServiceID.
- ServiceName.
- CorrelationRuleID.
- AggregationRuleID.

6. Нажмите **OK**.
7. В открывшемся окне подтверждения нажмите **OK**.

Партиции из стороннего экземпляра Kaspersky SIEM Cloud будут импортированы. Также будут созданы задача импорта партиций и событие аудита.

Настройка хранилища S3

Kaspersky SIEM Cloud позволяет сохранять экспортируемые события в собственном хранилище S3. Для этого нужно предварительно настроить подключение к нему. После настройки пользователи с соответствующими правами смогут экспортировать события из раздела **Поиск угроз** в настроенное хранилище.

Чтобы настроить хранилище S3:

1. В веб-консоли перейдите в раздел **Параметры** → **Хранилище S3**.
2. Укажите значения для следующих параметров:
   a. В поле **Секрет** укажите секрет для доступа к хранилищу S3. Вы можете выбрать секрет в раскрывающемся списке или создать новый секрет, нажав **Создать**.
   b. В поле **Цепочка сертификатов** укажите путь к файлу с полной цепочкой доверия сертификатов для подключения к хранилищу S3.

      Поле нужно заполнить, если для подключения к хранилищу S3 используется протокол HTTPS. Если используется HTTP, указывать сертификат не требуется.

      При использовании Huawei Cloud Object Storage Service нужно обязательно загрузить доверенные сертификаты.

   c. В поле **Имя бакета** укажите имя бакета, в который нужно сохранять экспортируемые файлы.

Допустимые символы и правила формирования имени бакета зависят от поставщика хранилища S3. Перед заполнением поля проверьте требования к именованию бакетов в используемом сервисе.

Общие рекомендации по указанию имени бакета:

- длина – от 3 до 63 символов;
- может содержать строчные буквы латинского алфавита, цифры и дефисы;
- первый символ – буква, последний – не дефис и не точка;
- не может содержать точку и дефис рядом;
- не может содержать две точки или два дефиса подряд.

d. В поле **Путь** укажите путь к каталогу внутри бакета, в котором будут сохраняться экспортируемые файлы. Путь должен начинаться с прямой косой черты (`/`).

Пример

```
/exports/events
```

Ограничения:

- Длина пути, включая имя экспортируемого файла, не должна превышать 1024 байта.
- В качестве разделителя каталогов используется прямая косая черта (`/`).
- Путь не может содержать два прямые косые черты подряд (`//`).
- Путь не может содержать следующие специальные символы: `\`, `:`, `*`, `?`, `"`, `<`, `>`, `|`.

e. Проверьте значения автоматически заполненных параметров:

a. **Идентификатор региона** – регион размещения бакета.

b. **Конечное устройство** – адрес конечного устройства хранилища S3.

c. **URL бакета** – полный адрес, по которому будут сохраняться экспортируемые файлы.

Значение поля **URL бакета** формируется на основании значений полей **Имя бакета**, **Путь**, **Идентификатор региона** и **Конечное устройство**.

Пример

```
https://<bucket_name>.<region_ID>.<endpoint_address><directory_path>
```

где:

- `<bucket_name>` – имя бакета;
- `<region_ID>` – идентификатор региона;

- `<endpoint_address>` – адрес конечного устройства хранилища S3;
- `<directory_path>` – путь к каталогу внутри бакета.

3. Проверьте соединение с хранилищем, нажав на кнопку **Проверить подключение**.
4. Нажмите на кнопку **Сохранить подключение**.

Хранилище S3 будет настроено и доступно для экспорта событий.

Настройка сроков хранения и приоритетного удаления событий

Если в Kaspersky SIEM Cloud нужно хранить события, связанные с обнаруженными инцидентами информационной безопасности, в течение более длительного срока, чем остальные события, можно настроить для них отдельное пространство хранилища.

В Kaspersky SIEM Cloud для каждого пространства предусмотрено одно хранилище – **[OOTB] OSMP Storage**. Для хранения корреляционных событий нужно добавить в это хранилище отдельное пространство с фильтром, который выбирает корреляционные события, и задать для него нужный срок хранения.

> События, связанные с инцидентами вручную, не попадают в отдельное пространство по этому механизму. Настройка распространяется на корреляционные события, создаваемые коррелятором.

Чтобы настроить срок хранения корреляционных событий:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Хранилища**.
2. Откройте параметры хранилища **[OOTB] OSMP Storage**.
3. В блоке параметров **Пространства** нажмите на кнопку **Добавить пространство** и укажите следующие параметры для первого пространства:
   a. В поле **Название** укажите `retention_180`.
   b. В блоке параметров **Варианты условий хранения** в раскрывающемся списке выберите **Дни** и укажите `180`.
   c. В блоке параметров **Параметры фильтра** укажите условие `Type = 3`.

   В результате для нового пространства будут настроены фильтр, выбирающий корреляционные события, и срок их хранения – 180 дней.

   Убедитесь, что новое пространство находится на первом месте в списке пространств. При распределении событий хранилище проверяет пространства в порядке их следования в списке и помещает событие в первое пространство, фильтру которого оно соответствует.

   В хранилище **[OOTB] OSMP Storage** уже настроены пространства **edr**, **osmp-scanner** и **osmp-technical-events** с фильтрами по полям решения. Корреляционные события могут содержать такие же поля, поэтому без изменения порядка они могут попасть в одно из этих пространств вместо `retention_180`.

4. Нажмите на кнопку **Сохранить**.

5. Перезапустите сервис хранилища, чтобы применить изменения и создать новое пространство.

После настройки проверьте, что корреляционные события попадают в пространство `retention_180`:

1. Отправьте тестовые события, на основании которых предустановленный коррелятор сформирует корреляционное событие с условием `Type = 3`.

2. Убедитесь, что созданное корреляционное событие попало в пространство `retention_180`.

3. Убедитесь, что для этого пространства установлен срок хранения 180 дней.

Корреляционные события, создаваемые коррелятором, будут храниться в отдельном пространстве в течение 180 дней. Остальные события продолжат распределяться по пространствам хранилища в соответствии с настроенными для них фильтрами и условиями хранения.

Прием и нормализация событий

Коллектор является компонентом решения, предназначенным для приема событий из источников, их обработки и передачи в другие компоненты решения. В процессе обработки коллектор выполняет нормализацию событий, а также может применять фильтрацию, обогащение, преобразование и агрегацию данных. После обработки события передаются в настроенные точки назначения.

Максимальный размер события, обрабатываемого коллектором Kaspersky SIEM Cloud: 4 МБ.

> Если вы используете лицензию SMB и для коллектора превышено одновременно среднечасовое и среднесуточное количество EPS, допустимое лицензией, коллектор останавливает прием событий и отображается с красным статусом и уведомлением о превышении лимита EPS. Пользователю с ролью Главный администратор будет отправлено уведомление о превышении лимита EPS и остановке коллектора. Каждый час происходит подсчет среднечасового значения EPS и полученное значение сравнивается с лимитом EPS в лицензии. Если среднечасовое значение ниже лимита, ограничения на коллекторе будут сняты и коллектор восстановит прием и обработку событий.

Для каждого коллектора нужно настроить один коннектор и один нормализатор. Вы также можете настроить любое количество дополнительных нормализаторов, фильтров, правил обогащения и правил агрегации. Для того чтобы коллектор мог отправлять нормализованные события в другие сервисы, необходимо добавить точки назначения. Как правило, используются две точки назначения: хранилище и коррелятор.

Коллектор предназначен для приема сырых событий из источников событий, дальнейшей нормализации и передачи обработанных событий в точки назначения.

Предустановленные коллекторы

В поставку Kaspersky SIEM Cloud включены следующие предустановленные коллекторы:

- [OOTB] CEF – собирает события в формате CEF, поступающие по протоколу TCP.
- [OOTB] KSC – собирает события от Kaspersky Security Center по протоколу Syslog TCP.

- [OOTB] KSC SQL – собирает события от Kaspersky Security Center с использование запроса к базе данных MS SQL.
- [OOTB] Syslog – собирает события по протоколу Syslog.
- [OOTB] Syslog-CEF – собирает события в формате CEF, поступающих по протоколу UDP и имеющих заголовок Syslog.

Рекомендации для ресурсов коллектора

Для эффективной обработки событий коллектором количество ядер процессора важнее, чем их частота. Например, восемь ядер процессора со средней частотой будут эффективнее обрабатывать события, чем четыре ядра с высокой частотой.

Также необходимо иметь в виду, что количество потребляемой коллектором оперативной памяти зависит от настроенных методов обогащения (DNS, учетные записи, активы) и использования агрегации (на потребление оперативной памяти влияет параметр окна агрегации данных, количество полей, по которым выполняется агрегация данных, объем данных в агрегируемых полях). Показатели использования Kaspersky SIEM Cloud вычислительных ресурсов зависят от типа анализируемых событий и от эффективности нормализатора.

Например, при потоке событий 1000 EPS и выключенном обогащении событий (обогащение событий выключено, агрегация событий выключена, 5000 учетных записей, 5000 активов в тенанте) одному коллектору требуются следующие ресурсы:

- 1 процессорное ядро или 1 виртуальный процессор;
- 512 МБ оперативной памяти;
- 1 ГБ свободного дискового пространства (без учета кеша событий).

Например, для пяти коллекторов, которые не выполняют обогащение событий потребуется выделить следующие ресурсы: 5 процессорных ядер, 2,5 ГБ оперативной памяти и 5 ГБ свободного дискового пространства.

Алгоритм работы коллектора

Алгоритм работы коллектора состоит из следующих этапов:

1. Получение сообщений из источников событий

Коллектор получает сообщения из источников событий через коннекторы. В зависимости от типа коннектора получение данных может выполняться двумя способами:

- пассивный коннектор ожидает поступления событий от источника;
- активный коннектор самостоятельно инициирует подключение к источнику.

Тип коннектора определяется используемым транспортным протоколом обмена данными.

2 Парсинг и нормализация событий

Полученные сообщения обрабатываются нормализатором и правилами нормализации. В процессе обработки данные из исходного формата преобразуются в унифицированное представление события. Используемый нормализатор определяется форматом входящих сообщений.

3 Фильтрация нормализованных событий

Нормализованные события проверяются на соответствие условиям фильтрации. События, удовлетворяющие заданным условиям, передаются на последующие этапы обработки.

4 Обогащение и преобразование нормализованных событий

На этапе обогащения события дополняются данными из внутренних и внешних источников.

На этапе преобразования значения полей события изменяются в соответствии с заданными правилами преобразования.

5 Агрегация нормализованных событий

Схожие события могут объединяться в одно агрегированное событие в соответствии с правилами агрегации. Это позволяет уменьшить объем передаваемых и хранимых данных, снизить нагрузку на сервисы дальнейшей обработки и сократить потребление лицензионной квоты (EPS). Например, несколько событий сетевых подключений между двумя IP-адресами, полученных за определенный интервал времени, могут быть объединены в одно событие.

6 Передача нормализованных событий

После завершения всех этапов обработки событие передается в настроенные точки назначения для дальнейшего хранения.

Поддерживаемые источники событий

Kaspersky SIEM Cloud поддерживает нормализацию событий, которые поступают от систем, перечисленных в таблице ниже. Нормализаторы для указанных систем включены в поставку.

Название системы	Название нормализатора	Тип	Описание нормализатора
1C EventJournal	[OOTB] 1C EventJournal Normalizer	xml	Предназначен для обработки журнала событий системы 1С. Источник событий – журнал регистрации 1С.
1C TechJournal	[OOTB] 1C TechJournal Normalizer	regexp	Предназначен для обработки технологического журнала событий. Источник событий – технологический журнал 1С.
Absolute Data and Device Security (DDS)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
AhnLab Malware Defense System (MDS)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
AhnLab UTM	[OOTB] Ahnlab UTM	regexp	Предназначен для обработки событий от системы Ahnlab. Источник событий – системные, операционные журналы, подключения, модуль IPS.
Alcatel AOS-W	[OOTB] Alcatel AOS-W syslog	regexp	Предназначен для обработки части событий, поступающих от системы Alcatel AOS-W версии 6.4 по Syslog.
Alcatel Network Switch	[OOTB] Alcatel Network Switch syslog	Syslog	Предназначен для обработки типов событий, полученных от сетевых коммутаторов Alcatel по Syslog.
Ansible	[OOTB] Ansible syslog	Syslog	Предназначен для обработки событий, поступающих от системы Ansible (версия 2.10.8) по Syslog.
Apache Cassandra	[OOTB] Apache Cassandra file	regexp	Предназначен для обработки событий в журналах СУБД Apache Cassandra версии 4.0.
Apache Kafka	[OOTB] Apache Kafka syslog	regexp	Предназначен для обработки событий аудита системы Apache Kafka версии 3.8.1, поступающих по Syslog.
Apache Tomcat	[OOTB] Apache Tomcat json	Syslog	Предназначен для обработки событий, поступающих от системы Apache Tomcat (версии 9.0 и выше, 10.1 и выше, 11.0 и выше) по Syslog в форматах JSON и key-value.
APC Smart-UPS	[OOTB] APC Smart UPS	regexp	Предназначен для обработки событий аудита системы APC Smart-UPS.
Aruba ClearPass	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Atlassian Confluence	[OOTB] Atlassian Jira Conflunce file	regexp	Предназначен для обработки событий систем Atlassian Jira, Atlassian Confluence (Jira версия 9.12, Confluence версия 8.5), хранящихся в файлах.
Atlassian Jira	[OOTB] Atlassian Jira Conflunce file	regexp	Предназначен для обработки событий систем Atlassian Jira, Atlassian Confluence (Jira версия 9.12, Confluence версия 8.5), хранящихся в файлах.
Avanpost FAM	[OOTB] Avanpost FAM syslog	regexp	Предназначен для обработки событий системы Avanpost Federated Access Manager (FAM) версии 1.9, поступающих по Syslog.
Avanpost IDM	[OOTB] Avanpost IDM syslog	regexp	Предназначен для обработки событий системы Avanpost IDM, поступающих по Syslog.
Avanpost PKI	[OOTB] Avanpost PKI syslog CEF	Syslog	Предназначен для обработки событий, поступающих от Avanpost PKI версии 6.0 в формате CEF по Syslog.
Avaya Aura Communication Manager	[OOTB] Avaya Aura Communication Manager syslog	regexp	Предназначен для обработки части событий, поступающих от системы Avaya Aura Communication Manager версии 7.1 по Syslog.
Avigilon Access Control Manager (ACM)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Ayehu eyeShare	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Arbor Pravail	[OOTB] Arbor Pravail syslog	Syslog	Предназначен для обработки событий системы Arbor Pravail, поступающих по Syslog.

Название системы	Название нормализатора	Тип	Описание нормализатора
Aruba Aruba AOS-S	[OOTB] Aruba Aruba AOS-S syslog	regexp	Предназначен для обработки типов событий, поступающих от сетевых устройств Aruba с прошивкой Aruba AOS-S версии 16.10 по Syslog. Нормализатор поддерживает обработку следующих типов событий: accounting events, ACL events, ARP protect events, authentication events, console events, loop protect events.
Barracuda Cloud Email Security Gateway	[OOTB] Barracuda Cloud Email Security Gateway syslog	regexp	Предназначен для обработки событий, поступающих от системы Barracuda Cloud Email Security Gateway по Syslog.
Barracuda Networks NG Firewall	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Barracuda Web Security Gateway	[OOTB] Barracuda Web Security Gateway syslog	Syslog	Предназначен для обработки части событий, поступающих от системы Barracuda Web Security Gateway версии 15.0 по Syslog.
BeyondTrust Privilege Management Console	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
BeyondTrust BeyondInsight	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Bifit Mitigator	[OOTB] Bifit Mitigator Syslog	Syslog	Предназначен для обработки событий от системы защиты от DDOS Mitigator, поступающих по Syslog.
Bloombase StoreSafe	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
BMC CorreLog	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Bricata ProAccel	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Brinqa Risk Analytics	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Broadcom Symantec Advanced Threat Protection (ATP)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Broadcom Symantec Endpoint Protection	[OOTB] Broadcom Symantec Endpoint Protection	regexp	Предназначен для обработки событий от системы Symantec Endpoint Protection.
Broadcom Symantec Endpoint Protection Mobile	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Broadcom Symantec Threat Hunting Center	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Brocade Fabric OS	[OOTB] Brocade Fabric OS syslog	Syslog	Предназначен для обработки событий Brocade Fabric OS версии 9.1, поступающих по Syslog.
Canonical LXD	[OOTB] Canonical LXD syslog	Syslog	Предназначен для обработки событий, поступающих по Syslog от системы Canonical LXD версии 5.18.
Check Point	[OOTB] Checkpoint syslog	Syslog	Предназначен для обработки событий, поступающих от межсетевого экрана Check Point версии R81 по Syslog.
Cisco Access Control Server (ACS)	[OOTB] Cisco ACS syslog	regexp	Предназначен для обработки событий системы Cisco Access Control Server (ACS), поступающих по Syslog.

Название системы	Название нормализатора	Тип	Описание нормализатора
Cisco ACE	[OOTB] Cisco ASA and IOS syslog	regexp	Предназначен для обработки событий аудита, поступающих от сетевых устройств Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE и устройств под управлением Cisco IOS по Syslog.
Cisco ASA	[OOTB] Cisco ASA and IOS syslog	Syslog	Предназначен для обработки событий аудита, поступающих от сетевых устройств Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE и устройств под управлением Cisco IOS по Syslog.
Cisco Email Security Appliance (WSA)	[OOTB] Cisco WSA AccessFile	regexp	Предназначен для обработки журнала событий прокси-сервера Cisco Email Security Appliance (WSA) версии 14.2, файл access.log.
Cisco ESA syslog	[OOTB] Cisco ESA syslog	Syslog	Предназначен для обработки типов событий, полученных от Cisco ESA версии 16.0 по Syslog.
Cisco Firepower Threat Defense	[OOTB] Cisco ASA and IOS syslog	Syslog	Предназначен для обработки событий аудита, поступающих от сетевых устройств Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE и устройств под управлением Cisco IOS по Syslog.
Cisco Firewall Services Module (FWSM)	[OOTB] Cisco ASA and IOS syslog	Syslog	Предназначен для обработки событий аудита, поступающих от сетевых устройств Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE и устройств под управлением Cisco IOS по Syslog.
Cisco Identity Services Engine (ISE)	[OOTB] Cisco ISE syslog	regexp	Предназначен для обработки событий системы Cisco Identity Services Engine (ISE) версии 3.2, поступающих по Syslog.
Cisco IOS	[OOTB] Cisco ASA and IOS syslog	Syslog	Предназначен для обработки событий аудита, поступающих от сетевых устройств Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE и устройств под управлением Cisco IOS по Syslog.
Cisco Netflow v5	[OOTB] NetFlow v5	netflow5	Предназначен для обработки событий, поступающих Cisco Netflow версии 5.
Cisco NetFlow v9	[OOTB] NetFlow v9	netflow9	Предназначен для обработки событий, поступающих Cisco Netflow версии 9.
Cisco Next-Generation Intrusion Prevention System (NGIPS)	[OOTB] Cisco ASA and IOS syslog	Syslog	Предназначен для обработки событий аудита, поступающих от сетевых устройств Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE и устройств под управлением Cisco IOS по Syslog.
Cisco PIX	[OOTB] Cisco ASA and IOS syslog	regexp	Предназначен для обработки типов событий аудита, поступающих от сетевых устройств Cisco ASA, FTD, FWSM, NGIPS, PIX, ACE и устройств под управлением Cisco IOS по Syslog.
Cisco Prime	[OOTB] Cisco Prime syslog	Syslog	Предназначен для обработки событий системы Cisco Prime версии 3.10, поступающих по Syslog.
Cisco Secure Email Gateway (SEG)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Cisco Secure Firewall Management Center	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Cisco Unified Communications Manager	[OOTB] Cisco Unified Communications Manager	regexp	Предназначен для обработки типов событий, поступающих от системы Cisco Unified Communications Manager версии 11.5.1.
Cisco Wireless LAN Controllers (WLCs)	[OOTB] Cisco WLC syslog	regexp	Предназначен для обработки типов событий, поступающих от сетевых устройств Cisco WLCs (2500 Series Wireless Controllers, 5500 Series Wireless Controllers, 8500 Series Wireless Controllers, Flex 7500 Series Wireless Controllers) по Syslog.
Cisco Web Security Appliance (WSA)	[OOTB] Cisco WSA file, [OOTB] Cisco WSA syslog	regexp	[OOTB] Cisco WSA file – нормализатор, который предназначен для обработки журнала событий прокси-сервера Cisco WSA (версии 14.2, 15.0). Нормализатор поддерживает обработку событий, сформированных с использованием шаблона: %t %e %a %w/%h %s %2r %A %H/%d %c %D %Xr %?BLOCK_SUSPECT_USER_AGENT,MONITOR_SUSPECT_USER_AGENT?%<User-Agent:%!%-%. %) %q %k %u %m [OOTB] Cisco WSA syslog – нормализатор, который предназначен для обработки событий, поступающих от системы Cisco WSA (версия 15.0) по Syslog.

Название системы	Название нормализатора	Тип	Описание нормализатора
Citrix NetScaler	[OOTB] Citrix NetScaler syslog	regexp	Предназначен для обработки событий, поступающих от балансировщика нагрузки Citrix NetScaler версии 13.7, Citrix ADC версии NS13.0.
Claroty Continuous Threat Detection	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
CloudPassage Halo	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Codemaster Mirada	[OOTB] Codemaster Mirada syslog	Syslog	Предназначен для обработки событий системы Codemaster Mirada, поступающих по Syslog.
CollabNet Subversion Edge	[OOTB] CollabNet Subversion Edge syslog	Syslog	Предназначен для обработки событий, поступающих от системы Subversion Edge (версия 6.0.2) по Syslog.
CommuniGate Pro	[OOTB] CommuniGate Pro	regexp	Содержит набор ресурсов для обработки части событий модуля SIP системы CommuniGate Pro версии 6.1 и 6.5.1, передаваемых агентом Kaspersky SIEM Cloud по протоколу TCP. Подробнее о настройке коллектора см. Создание коллектора.
Corvil Network Analytics	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Cribl Stream	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
CrowdStrike Falcon	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
CyberArk Privileged Threat Analytics (PTA)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
CyberPeak Spektr	[OOTB] CyberPeak Spektr syslog	Syslog	Предназначен для обработки событий системы CyberPeak Spektr версии 3, поступающих по Syslog.
Cyberprotect Cyber Backup	[OOTB] Cyberprotect Cyber Backup SQL [OOTB] Cyberprotect Cyber Backup syslog	sql, regexp	[OOTB] Cyberprotect Cyber Backup SQL – нормализатор, предназначенный для обработки событий, полученных коннектором из базы данных системы Кибер Бэкап (версия 16.5). [OOTB] Cyberprotect Cyber Backup syslog – нормализатор, предназначенный для обработки событий, поступающих в формате CEF от системы Кибер Бэкап (версия 17.2, 17.3, 18.5) по Syslog.
Deep Instinct	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Delinea Secret Server	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Dell Network Switch	[OOTB] Dell Network Switch syslog	regexp	Предназначен для обработки типов событий, полученных от сетевых коммутаторов Dell по Syslog.
Digital Guardian Endpoint Threat Detection	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
D-Link Switchesr	[OOTB] D-Link Switches	regexp	Предназначен для обработки событий, поступающих от коммутаторов D-Link (DES-2108, DES-3200-28, DES-3828, DES-3800) по Syslog.
DNS сервер BIND	[OOTB] BIND Syslog [OOTB] BIND file	Syslog regexp	[OOTB] BIND Syslog предназначен для обработки событий DNS-сервера BIND, поступающих по Syslog. [OOTB] BIND file предназначен для обработки журналов событий DNS-сервера BIND.
Docsvision	[OOTB] Docsvision syslog	Syslog	Предназначен для обработки событий аудита, поступающих от системы Docsvision по Syslog.
Dovecot	[OOTB] Dovecot Syslog	Syslog	Предназначен для обработки событий почтового сервера Dovecot, поступающих по Syslog. Источник событий – журналы POP3/IMAP.

Название системы	Название нормализатора	Тип	Описание нормализатора
Dragos Platform	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Dr.Web Enterprise Security Suite	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий Dr.Web Enterprise Security Suite версии 13.0.1 в формате CEF.
EclecticIQ Threat Intelligence Platform	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Edge Technologies AppBoard and enPortal	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Eltex ESR	[OOTB] Eltex ESR syslog	Syslog	Предназначен для обработки части событий, поступающих от сетевых устройств Eltex ESR по Syslog.
Eltex MES	[OOTB] Eltex MES syslog	regexp	Предназначен для обработки событий, поступающих от сетевых устройств Eltex MES (поддерживаемые модели устройств: MES14xx, MES24xx, MES3708P) по Syslog.
ESET PROTECT	[OOTB] ESET Protect syslog CEF	Syslog	Предназначен для обработки событий, поступающих в формате CEF от системы ESET PROTECT (версия 11.0) по Syslog.
Extreme Networks Summit Wireless Controller	[OOTB] Extreme Networks Summit Wireless Controller	regexp	Предназначен для обработки событий аудита устройства Extreme Networks Summit Wireless Controller (модель: WM3700, версия прошивки: 5.5.5.0–018R).
Factor-TS Dionis NX	[OOTB] Factor-TS Dionis NX syslog	regexp	Предназначен для обработки событий аудита, поступающих от системы Dionis NX (версия 2.0.3) по Syslog.
F5 Advanced Web Application Firewall	[OOTB] F5 Advanced Web Application Firewall syslog	regexp	Предназначен для обработки событий аудита, поступающих от системы F5 Advanced Web Application Firewall по Syslog.
F5 BigIP Advanced Firewall Manager (AFM)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
FFRI FFR yarai	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
FireEye CM Series	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
FireEye Malware Protection System	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Flant Deckhouse	[OOTB] Flant Deckhouse json	json	Предназначен для обработки событий аудита уровня Metadata системы Deckhouse (версия 1.67) в формате JSON.
Forcepoint NGFW	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Forcepoint SMC	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Fortinet FortiAnalyzer	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий, поступающих от системы Fortinet FortiAnalyzer версии 7.0, 7.2 по Syslog в формате CEF.
Fortinet FortiADC	[OOTB] FortiADC syslog KV	regexp	Предназначен для обработки типов событий, поступающих от балансировщиков нагрузки Fortinet FortiADC версии 7.1 по Syslog в формате key-value.
Fortinet FortiGate	[OOTB] FortiGate syslog KV [OOTB] FortiGate syslog CEF	regexp	[OOTB] FortiGate syslog KV – нормализатор, который предназначен для обработки событий, поступающих от межсетевых экранов FortiGate (версии 7.0, 7.2) по syslog. Источник событий – журналы FortiGate в формате key-value. [OOTB] FortiGate syslog CEF – нормализатор, который предназначен для обработки событий, поступающих от системы Fortinet FortiGate (версия FortiOS 6.4) по syslog в формате CEF.
Fortinet FortiMail	[OOTB] Fortimail	regexp	Предназначен для обработки событий системы защиты электронной почты FortiMail. Источник событий – журналы почтовой системы FortiMail.

Название системы	Название нормализатора	Тип	Описание нормализатора
Fortinet FortiPAM	[OOTB] Fortinet FortiPAM syslog	regexp	Предназначен для обработки событий, поступающих от системы Fortinet FortiPAM (версия 7.4) в формате key-value по протоколу Syslog.
Fortinet FortiSOAR	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Fortinet FortiWeb	[OOTB] FortiNet FortiWeb CEF	Syslog	Предназначен для обработки событий, поступающих от системы Fortinet FortiWeb (версии 7.6.1) в формате CEF.
FreeBSD	[OOTB] FreeBSD file	regexp	Предназначен для обработки событий операционной системы FreeBSD (версия 13.1-RELEASE), хранящихся в файле. Нормализатор поддерживает обработку файлов, полученных в результате работы утилиты praudit. Пример: praudit -xl /var/audit/AUDITFILE >> file_name.log
FreeIPA	[OOTB] FreeIPA	json	Предназначен для обработки событий, поступающих от системы FreeIPA. Источник событий – журналы службы каталогов FreeIPA.
FreeRADIUS	[OOTB] FreeRADIUS syslog	Syslog	Предназначен для обработки событий системы FreeRADIUS, поступающих по Syslog. Нормализатор поддерживает события от FreeRADIUS версии 3.0.
GajShield Firewall	[OOTB] GajShield Firewall syslog	regexp	Предназначен для обработки части событий, поступающих от системы GajShield Firewall версии GAJ_OS_Bulwark_Firmware_v4.35 по Syslog.
Garda Monitor	[OOTB] Garda Monitor syslog	Syslog	Предназначен для обработки событий системы Garda Monitor версии 3.4, поступающих по Syslog.
Gardatech Garda DB	[OOTB] Gardatech GardaDB syslog	Syslog	Предназначен для обработки событий системы Gardatech Perimeter версии 5.3, 5.4, поступающих по Syslog.
Gardatech Perimeter	[OOTB] Gardatech Perimeter syslog	Syslog	Предназначен для обработки событий системы Gardatech Perimeter версии 5.3, поступающих по Syslog.
Gigamon GigaVUE	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Grafana	[OOTB] Grafana syslog json	Syslog	Предназначен для обработки событий, поступающих от системы Grafana версии 9.5.15 в формате JSON по Syslog.
HAProxy	[OOTB] HAProxy syslog	Syslog	Предназначен для обработки событий, поступающих от HAProxy версии 2.4 по Syslog. Нормализатор поддерживает обработку событий в форматах Default, TCP, TCP CLF (версии 3.2 и выше), HTTP, HTTP CLF, HTTPS (версии 2.6 и выше) и Error.
HashiCorp Vault	[OOTB] HashiCorp Vault json	json	Предназначен для обработки событий, поступающих от системы HashiCorp Vault версии 1.16 в формате JSON.
Huawei Eudemon	[OOTB] Huawei Eudemon	regexp	Предназначен для обработки событий, поступающих от межсетевых экранов Huawei Eudemon. Источник событий – журналы межсетевых экранов Huawei Eudemon.
Huawei iManager 2000	[OOTB] Huawei iManager 2000 file	regexp	Предназначен для обработки части событий системы Huawei iManager 2000, хранящихся в файлах \client\logs\rpc, \client\logs\deploy\ossDeployment.
Huawei USG	[OOTB] Huawei USG Basic	Syslog	Предназначен для обработки событий, поступающих от шлюзов безопасности Huawei USG по Syslog.
Huawei VRP	[OOTB] Huawei VRP syslog	regexp	Предназначен для обработки типов событий системы Huawei VRP, поступающих по Syslog. Нормализатор осуществляет выборку части данных из событий.
IBM InfoSphere Guardium	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Ideco UTM	[OOTB] Ideco UTM Syslog	Syslog	Предназначен для обработки событий, поступающих от Ideco UTM по Syslog. Нормализатор поддерживает обработку событий Ideco UTM версии 14.7, 14.10, 17.5.
Illumio Policy Compute Engine (PCE)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.

Название системы	Название нормализатора	Тип	Описание нормализатора
Imperva Incapsula	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Imperva SecureSphere	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Indeed Access Manager	[OOTB] Indeed Access Manager syslog	Syslog	Предназначен для обработки событий, поступающих от системы Indeed Access Manager по Syslog.
Indeed Privileged Access Manager	[OOTB] Indeed PAM syslog [OOTB] Indeed PAM syslog CEF	Syslog	Нормализатор [OOTB] Indeed PAM syslog предназначен для обработки событий, поступающих от системы Indeed Privileged Access Manager версии 2.6. Нормализатор [OOTB] Indeed PAM syslog CEF предназначен для обработки событий, поступающих от системы Indeed Privileged Access Manager (версия 3.3) в формате CEF по Syslog.
Indeed SSO	[OOTB] Indeed SSO xml	xml	Предназначен для обработки событий системы Indeed SSO (Single Sign-On).
InfoWatch Person Monitor	[OOTB] InfoWatch Person Monitor SQL	sql	Предназначен для обработки системных событий аудита из СУБД MS SQL системы InfoWatch Person Monitor версии 10.2.
InfoWatch Traffic Monitor	[OOTB] InfoWatch Traffic Monitor SQL	sql	Предназначен для обработки событий, полученных коннектором из базы данных системы InfoWatch Traffic Monitor.
Intralinks VIA	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
IPFIX	[OOTB] IPFIX	ipfix	Предназначен для обработки событий в формате IP Flow Information Export (IPFIX).
Juniper JUNOS	[OOTB] Juniper-JUNOS	regexp	Нормализатор для событий Juniper JUNOS (версия 24.2), поступающих по Syslog.
Kaspersky Anti Targeted Attack (KATA)	[OOTB] KATA	cef	Предназначен для обработки алертов или событий из журнала активности Kaspersky Anti Targeted Attack.
Kaspersky CyberTrace	[OOTB] CyberTrace	regexp	Предназначен для обработки событий Kaspersky CyberTrace.
Kaspersky DFI	[OOTB] Kaspersky DFI json	json	Предназначен для обработки событий аудита системы Kaspersky DFI в формате JSON. Нормализатор поддерживает обработку событий, сформированных коннектором Kaspersky SIEM Cloud "dfi".
Kaspersky Endpoint Detection and Response (KEDR)	[OOTB] KEDR telemetry	json	Предназначен для обработки телеметрии Kaspersky EDR, размеченных KATA. Источник событий – kafka, EnrichedEventTopic.
Kaspersky Endpoint Security for Linux	[OOTB] KESL syslog cef [OOTB] KESL json	Syslog, json	[OOTB] KESL syslog cef – нормализатор, который предназначен для обработки событий, поступающих от Kaspersky Endpoint Security for Linux (KESL) версии 12.2 в формате CEF по syslog. [OOTB] KESL json – нормализатор, который предназначен для обработки событий, поступающих от Kaspersky Endpoint Security for Linux (KESL) версии 12.5 в формате JSON.
KICS/KATA	[OOTB] KICS4Net v2.x	cef	Предназначен для обработки событий KICS/KATA версии 2.x.
KICS/KATA	[OOTB] KICS4Net v3.x	Syslog	Предназначен для обработки событий KICS/KATA версии 3.x.
Kaspersky Industrial CyberSecurity for Networks 4.2	[OOTB] Kaspersky Industrial CyberSecurity for Networks 4.2 syslog [OOTB] Kaspersky Industrial CyberSecurity for Networks 4.x syslog	Syslog	Нормализатор [OOTB] Kaspersky Industrial CyberSecurity for Networks 4.2 syslog предназначен для обработки событий, поступающих от системы Kaspersky Industrial CyberSecurity for Networks версии 4.2 по Syslog. Этот нормализатор устарел. Рекомендуется использовать нормализатор [OOTB] Kaspersky Industrial CyberSecurity for Networks 4.x syslog.

Название системы	Название нормализатора	Тип	Описание нормализатора
Kaspersky Industrial CyberSecurity for Networks 4.2, 4.3, 4.5	[OOTB] Kaspersky Industrial CyberSecurity for Networks 4.x syslog	Syslog	Предназначен для обработки событий, поступающих от системы Kaspersky Industrial CyberSecurity for Networks версии 4.2, 4.3, 4.5 по Syslog.
Kaspersky IoT Secure Gateway (KISG)	[OOTB] Kaspersky KISG syslog	Syslog	Предназначен для обработки событий, поступающих от системы Kaspersky IoT Secure Gateway (KISG) версии 3.0 по Syslog.
Kaspersky NGFW	[OOTB] Kaspersky NGFW CEF	cef	Предназначен для обработки событий, поступающих от системы Kaspersky NGFW версии 1.0, 1.2 в формате CEF.
Kaspersky NDR	[OOTB] Kaspersky NDR syslog	Syslog	Предназначен для обработки событий, поступающих от системы Kaspersky NDR версии 7.0 по Syslog.
Open Single Management Platform	[OOTB] KSC	cef	Предназначен для обработки событий Open Single Management Platform в формате CEF.
Open Single Management Platform	[OOTB] KSC from SQL	sql	Предназначен для обработки событий, полученных коннектором из базы данных системы Open Single Management Platform.
Kaspersky Security for Linux Mail Server (KLMS)	[OOTB] KLMS Syslog CEF	Syslog	Предназначен для обработки событий, поступающих от Kaspersky Security for Linux Mail Server в формате CEF по Syslog.
Kaspersky Security for MS Exchange SQL	[OOTB] Kaspersky Security for MS Exchange SQL	sql	Предназначен для обработки событий системы Kaspersky Security for Exchange (KSE) версия 9.0, хранящихся в БД.
Kaspersky Secure Mail Gateway (KSMG)	[OOTB] KSMG syslog CEF [OOTB] KSMG 2.1+ syslog CEF	Syslog	[OOTB] KSMG syslog CEF – нормализатор для обработки событий KSMG версии 2.0 в формате CEF по Syslog. [OOTB] KSMG 2.1+ syslog CEF – нормализатор для обработки событий, поступающих от системы KSMG версии 2.1.1, 3.0 в формате CEF по Syslog.
KUMA	[OOTB] KUMA forwarding	json	Предназначен для обработки событий, перенаправленных из KUMA.
Kaspersky Web Traffic Security (KWTS)	[OOTB] KWTS Syslog CEF, [OOTB] KWTS (KV)	Syslog	[OOTB] KWTS Syslog CEF – нормализатор, который предназначен для обработки событий, поступающих от Kaspersky Web Traffic Security в формате CEF по Syslog. [OOTB] KWTS (KV) – нормализатор, который предназначен для обработки событий Kaspersky Web Traffic Security в формате key-value.
Keycloak	[OOTB] Keycloak syslog	Syslog	Предназначен для обработки событий аудита системы Keycloak версии 26.3, поступающих по Syslog.
Kemp Technologies LoadMaster	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Kerio Control	[OOTB] Kerio Control	Syslog	Предназначен для обработки событий межсетевых экранов Kerio Control.
LastLine Enterprise	[OOTB] LastLine Enterprise syslog cef	Syslog	Предназначен для обработки событий, поступающих от системы LastLine Enterprise версии 7.3, 8.1, 9.1 по Syslog в формате CEF.
Libvirt	[OOTB] Libvirt syslog	Syslog	Предназначен для обработки событий Libvirt версии 8.0.0, поступающих по Syslog.
Lieberman Software ERPM	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Linux	[OOTB] Linux audit and iptables Syslog v1	Syslog	Предназначен для обработки событий операционной системы Linux. Нормализатор не поддерживает обработку событий в формате ENRICHED.
Linux auditd	[OOTB] Linux auditd syslog for KUMA 3.2	Syslog	Предназначен для обработки событий аудита (пакет auditd) операционной системы Linux, поступающих по Syslog.

Название системы	Название нормализатора	Тип	Описание нормализатора
Linux auditd	[OOTB] Linux auditd file for KUMA 3.2	regexp	Предназначен для обработки событий аудита (пакет auditd) операционной системы Linux, хранящихся в файле.
MariaDB	[OOTB] MariaDB Audit Plugin Syslog	Syslog	Предназначен для обработки событий, поступающих от плагина аудита MariaDB Audit по Syslog.
McAfee Endpoint DLP	[OOTB] McAfee Endpoint DLP syslog	Syslog	Предназначен для обработки событий, поступающих от системы McAfee Endpoint DLP Windows версии 11.10.200 по Syslog.
McAfee Web Gateway	[OOTB] McAfee Web Gateway	regexp	Предназначен для обработки событий, поступающих от системы McAfee Web Gateway (версия 7.8 и выше) в форматах CEF и KV по Syslog.
Microsoft Active Directory Certificate Services (AD CS)	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий журнала Active Directory Certificate Services (AD CS) в формате XML.
Microsoft Active Directory Federation Service (AD FS)	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий Microsoft AD FS.
Microsoft Active Directory Domain Service (AD DS)	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий Microsoft AD DS.
Microsoft Defender	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий системы Microsoft Defender.
Microsoft DHCP	[OOTB] MS DHCP file	regexp	Предназначен для обработки событий от DHCP-сервера Microsoft. Источник событий – журналы DHCP сервера Windows.

Название системы	Название нормализатора	Тип	Описание нормализатора
Microsoft DNS	[OOTB] DNS Windows [OOTB] Microsoft DNS ETW logs json	regexp	Нормализатор [OOTB] DNS Windows предназначен для обработки событий DNS сервера Microsoft. Источник событий – журналы DNS сервера Windows. Нормализатор не поддерживает обработку событий журнала отладки с включенной опцией **Details**. Нормализатор [OOTB] Microsoft DNS ETW logs json предназначен для обработки части событий аудита Microsoft DNS Server, предоставляемых ETW-провайдером.
Microsoft Exchange Server	[OOTB] Exchange CSV	csv	Предназначен для обработки журнала событий системы Microsoft Exchange. Источник событий – журналы MTA сервера Exchange.
Microsoft Hyper-V	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий операционной системы Microsoft Windows. Источник событий – журналы Microsoft Hyper-V: Microsoft-Windows-Hyper-V-VMMS-Admin, Microsoft-Windows-Hyper-V-Compute-Operational, Microsoft-Windows-Hyper-V-Hypervisor-Operational, Microsoft-Windows-Hyper-V-StorageVSP-Admin, Microsoft-Windows-Hyper-V-Hypervisor-Admin, Microsoft-Windows-Hyper-V-VMMS-Operational, Microsoft-Windows-Hyper-V-Compute-Admin.
Microsoft Installer	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий журнала Microsoft Installer (MSI Installer) в формате XML.
Microsoft IIS	[OOTB] IIS Log File Format	regexp	Предназначен для обработки событий в формате, описанном по ссылке: https://learn.microsoft.com/en-us/windows/win32/http/iis-logging. Источник событий – журналы Microsoft IIS.
Microsoft Network Policy Server (NPS)	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий операционной системы Microsoft Windows. Источник событий – события Network Policy Server.
Microsoft Office 365	[OOTB] Microsoft Office 365 json	json	Предназначен для обработки типов событий аудита Microsoft Office 365. Нормализатор поддерживает обработку типов событий аудита, поступающих от систем Microsoft Teams, Azure Active Directory, SharePoint.
Microsoft SCCM	[OOTB] Microsoft SCCM file	regexp	Предназначен для обработки событий системы Microsoft SCCM версии 2309. Нормализатор поддерживает обработку части событий, хранящихся в файле AdminService.log.
Microsoft SharePoint Server	[OOTB] Microsoft SharePoint Server diagnostic log file	regexp	Предназначен для обработки части событий системы Microsoft SharePoint Server (версия SharePoint Server 2016), хранящихся в диагностических журналах.

Название системы	Название нормализатора	Тип	Описание нормализатора
Microsoft Sysmon	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий модуля Microsoft Sysmon.
Microsoft Windows 7, 8.1, 10, 11	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки части событий из журналов Security, System, Application операционной системы Microsoft Windows. Нормализатор [OOTB] Microsoft Products via KES WIN поддерживает ограниченное количество типов событий аудита, передаваемых в Kaspersky SIEM Cloud от Kaspersky Endpoint Security для Windows 12.6 по Syslog.
Microsoft → Windows → AppLocker	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий журнала Microsoft → Windows → AppLocker в формате XML.
Microsoft → Windows → DNS-Server → Audit	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий журнала Microsoft → Windows → DNS-Server → Audit в формате XML.
Microsoft → Windows → Group Policy → Operational	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий журнала Microsoft → Windows → Group Policy → Operational в формате XML.

Название системы	Название нормализатора	Тип	Описание нормализатора
Microsoft → Windows → PowerShell	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий журналов PowerShell операционной системы Microsoft Windows.
Microsoft → Windows → PowerShell-Operational	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий журналов PowerShell-Operational операционной системы Microsoft Windows. Нормализатор [OOTB] Microsoft Products via KES WIN поддерживает ограниченное количество типов событий аудита, передаваемых в Kaspersky SIEM Cloud от Kaspersky Endpoint Security для Windows 12.6 по Syslog.
Microsoft → Windows → System log → Netlogon	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий журнала Microsoft → Windows → System log → Netlogon в формате XML.
Microsoft → Windows → TaskScheduler → Operational	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий журнала Microsoft → Windows → TaskScheduler → Operational в формате XML.
Microsoft → Windows → WinRM → Operational	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий журнала Microsoft → Windows → WinRM → Operational в формате XML.

Название системы	Название нормализатора	Тип	Описание нормализатора
Microsoft SQL Server	[Deprecated] [OOTB] Microsoft SQL Server xml	xml	Предназначен для обработки событий MS SQL Server версии 2008, 2012, 2014, 2016.
Microsoft SQL Server, Microsoft SQL Server Express	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий MS SQL Server версии 2008 и новее.
Microsoft Windows Remote Desktop Services	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий операционной системы Microsoft Windows. Источник событий → журнал Applications and Services Logs → Microsoft → Windows → TerminalServices-LocalSessionManager → Operational. Нормализатор [OOTB] Microsoft Products via KES WIN поддерживает ограниченное количество типов событий аудита, передаваемых в Kaspersky SIEM Cloud от Kaspersky Endpoint Security для Windows 12.6 по Syslog.
Microsoft Windows Service Control Manager	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки событий журналов Service Control Manager (журнал System) операционной системы Microsoft Windows.
Microsoft Windows Server 2008 R2, 2012 R2, 2016, 2019, 2022	[OOTB] Microsoft Products [OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки части событий из журналов Security, System операционной системы Microsoft Windows Server. Нормализатор [OOTB] Microsoft Products via KES WIN поддерживает ограниченное количество типов событий аудита, передаваемых в Kaspersky SIEM Cloud от Kaspersky Endpoint Security для Windows 12.6 по Syslog.
Microsoft Windows XP/2003	[OOTB] SNMP. Windows {XP/2003}	json	Предназначен для обработки событий, поступающих от рабочих станций и серверов под управлением операционных систем Microsoft Windows XP, Microsoft Windows 2003 с использованием протокола SNMP.

Название системы	Название нормализатора	Тип	Описание нормализатора
Microsoft WSUS	[OOTB] Microsoft WSUS file	regexp	Предназначен для обработки событий системы Gardatech Perimeter версии 5.3, 5.4, поступающих по Syslog.
MikroTik	[OOTB] MikroTik syslog	regexp	Предназначен для событий, поступающих от устройств MikroTik по Syslog.
Minerva Labs Minerva EDR	[OOTB] Minerva EDR	regexp	Предназначен для обработки событий от EDR системы Minerva.
MongoDB	[OOTB] MongoDb syslog	Syslog	Предназначен для обработки части событий, поступающих от базы данных MongoDB версии 7.0 по Syslog.
Multifactor Radius Server for Windows	[OOTB] Multifactor Radius Server for Windows syslog	Syslog	Предназначен для обработки событий, поступающих от системы Multifactor Radius Server версии 1.0.2 для Microsoft Windows по протоколу Syslog.
MySQL 5.7	[OOTB] MariaDB Audit Plugin Syslog	Syslog	Предназначен для обработки событий, поступающих от плагина аудита MariaDB Audit по Syslog.
NetApp ONTAP (AFF, FAM)	[OOTB] NetApp syslog, [OOTB] NetApp file	regexp	[OOTB] NetApp syslog предназначен для обработки событий системы NetApp (версия – ONTAP 9.12), поступающих по Syslog. [OOTB] NetApp file предназначен для обработки событий системы NetApp (версия – ONTAP 9.12), хранящихся в файле.
NetApp SnapCenter	[OOTB] NetApp SnapCenter file	regexp	Предназначен для обработки части событий системы NetApp SnapCenter (версия SnapCenter Server 5.0). Нормализатор поддерживает обработку части событий из файла C:\Program Files\NetApp\SnapCenter WebApp\App_Data\log\napManagerWeb.*.log. Типы поддерживаемых событий в формате xml из файла SnapManagerWeb.*.log: SmDiscoverPluginRequest, SmDiscoverPluginResponse, SmGetDomainsResponse, SmGetHostPluginStatusRequest, SmGetHostPluginStatusResponse, SmGetHostRequest, SmGetHostResponse, SmRequest. Нормализатор поддерживает обработку части событий из файла C:\Program Files\NetApp\SnapCenter WebApp\App_Data\log\audit.log
Netgear Switch	[OOTB] Netgear Switch syslog	regexp	Предназначен для обработки событий аудита, поступающих от коммутатора Netgear (модель M4300-52G).
NetIQ Identity Manager	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
NetScout Systems nGenius Performance Manager	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Netskope Cloud Access Security Broker	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Netwrix Auditor	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Netwrix Endpoint Protector	[OOTB] Netwrix Endpoint Protector syslog	regexp	Предназначен для обработки событий, поступающих от системы Netwrix Endpoint Protector (версия 5.9) по Syslog.
Nextcloud	[OOTB] Nextcloud syslog	Syslog	Предназначен для событий Nextcloud версии 26.0.4, поступающих по Syslog. Нормализатор не сохраняет информацию из поля Trace.
Nexthink Engine	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
NFS kernel server	[OOTB] NFS kernel server syslog	regexp	Предназначен для обработки событий NFS kernel server (версии NFSv3, NFSv4.0, NFSv4.1, NFSv4.2) в формате Syslog.
Nginx	[OOTB] Nginx regexp	regexp	Предназначен для обработки журнала событий веб-сервера Nginx в формате Combined. Нормализатор поддерживает обработку событий, поступающих по Syslog и хранящихся в файле.
NIKSUN NetDetector	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
NPO Fractel	[OOTB] NPO Fractel SSPT-4	regexp	Предназначен для обработки событий системы НПО Фрактел ССПТ-4А1.

Название системы	Название нормализатора	Тип	Описание нормализатора
One Identity Privileged Session Management	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
OpenLDAP	[OOTB] OpenLDAP	regexp	Предназначен для построчной обработки части событий системы OpenLDAP версия 2.5, файл auditlog.ldif.
OpenVPN	[OOTB] OpenVPN file	regexp	Предназначен для обработки журнала системы OpenVPN.
Oracle	[OOTB] Oracle Audit Trail	sql	Предназначен для обработки событий аудита БД, полученных коннектором непосредственно из базы данных Oracle.
Orion soft Cloudlink	[OOTB] OrionSoft Cloudlink syslog	regexp	Предназначен для обработки событий, поступающих от системы Orion soft Cloudlink (версия 1.0) в формате CEF по Syslog.
Orion soft Termit	[OOTB] OrionSoft Termit syslog	Syslog	Предназначен для обработки событий, поступающих от системы Orion soft Termit версии 2.2, 2.3, 2.4 по Syslog.
Orion soft zVirt	[OOTB] Orion Soft zVirt syslog	regexp	Предназначен для обработки событий системы виртуализации Orion soft zVirt (версии zVirt 3.1, 4.4, 4.5, 5.0 и zVirt Max 1.2).
PagerDuty	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Palo Alto Cortex Data Lake	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Palo Alto Networks NGFW	[OOTB] Palo Alto NGFW syslog csv	Syslog	Предназначен для обработки событий от межсетевых экранов Palo Alto Networks, поступающих по Syslog в формате CSV.
Palo Alto Networks PANOS	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Parsec ParsecNet	[OOTB] Parsec ParsecNet	sql	Предназначен для обработки событий, полученных коннектором из базы данных системы Parsec ParsecNet версии 3.
Passwork	[OOTB] Passwork syslog	Syslog	Предназначен для обработки событий, поступающих от системы Passwork версии 050219 по Syslog.
Penta Security WAPPLES	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Positive Technologies ISIM	[OOTB] PTsecurity ISIM	regexp	Предназначен для обработки событий от системы PT Industrial Security Incident Manager.
Positive Technologies Network Attack Discovery (NAD)	[OOTB] PT NAD json	json	Предназначен для обработки событий, поступающий от PT NAD в формате json. Нормализатор поддерживает обработку событий PT NAD версий 11.1, 11.0.
Positive Technologies Multiscanner	[OOTB] PTsecurity Multiscanner json	Syslog	Предназначен для обработки событий, поступающих от системы PT Multiscanner (версия 5.24) формате JSON по Syslog.
Positive Technologies Sandbox	[OOTB] PTsecurity Sandbox	regexp	Предназначен для обработки событий системы PT Sandbox.
Positive Technologies Web Application Firewall	[OOTB] PTsecurity WAF syslog	Syslog	Предназначен для обработки событий, поступающих от системы PTsecurity Web Application Firewall версии 4 по Syslog.
Postfix	[OOTB] Postfix syslog	regexp	Содержит набор ресурсов для обработки событий Postfix версии 3.6. Поддерживается обработка Syslog-событий, поступающих по протоколу TCP.
PostgreSQL pgAudit	[OOTB] PostgreSQL pgAudit Syslog	Syslog	Предназначен для обработки событий плагина аудита pgAudit для базы данных PostgreSQL, поступающих по Syslog.
PowerDNS	[OOTB] PowerDNS syslog	Syslog	Предназначен для обработки событий PowerDNS Authoritative Server версии 4.5, поступающих по Syslog.
Proftpd	[OOTB] Proftpd syslog	regexp	Предназначен для обработки событий, поступающих от системы Proftpd версии 1.3.8c по Syslog.

Название системы	Название нормализатора	Тип	Описание нормализатора
Proofpoint Insider Threat Management	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Proxmox	[OOTB] Proxmox file	regexp	Предназначен для событий системы Proxmox версии 7.2-3, хранящихся в файле. Нормализатор поддерживает обработку событий в журналах access и pveam.
PT NAD	[OOTB] PT NAD json	json	Предназначен для обработки событий, поступающий от PT NAD в формате json. Нормализатор поддерживает обработку событий PT NAD версий 11.1, 11.0.
QEMU - журналы гипервизора	[OOTB] QEMU - Hypervisor file	regexp	Предназначен для обработки событий гипервизора QEMU, хранящихся в файле. Поддерживаются версии QEMU 6.2.0, Libvirt 8.0.0.
QEMU - журналы виртуальных машин	[OOTB] QEMU - Virtual Machine file	regexp	Предназначен для обработки событий из журналов виртуальных машин гипервизора QEMU версии 6.2.0, хранящихся в файле.
Radware DefensePro AntiDDoS	[OOTB] Radware DefensePro AntiDDoS	Syslog	Предназначен для обработки событий от системы защиты от DDOS Mitigator, поступающих по Syslog.
Reak Soft Blitz Identity Provider	[OOTB] Reak Soft Blitz Identity Provider file	regexp	Предназначен для обработки событий системы Reak Soft Blitz Identity Provider версии 5.16, хранящихся в файле.
RedCheck Desktop	[OOTB] RedCheck Desktop file	regexp	Предназначен для обработки журналов системы RedCheck Desktop версии 2.6, хранящихся в файле.
RedCheck WEB	[OOTB] RedCheck WEB file	regexp	Предназначен для обработки журналов системы RedCheck WEB версии 2.6, хранящихся в файлах.
RED SOFT RED ADM	[OOTB] RED SOFT RED ADM syslog	regexp	Предназначен для обработки событий, поступающих от системы RED ADM (версия РЕД АДМ: Промышленная редакция 1.1) по Syslog. Нормализатор поддерживает обработку событий: • подсистемы управления; • контроллера.
ReversingLabs N1000 Appliance	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Rubicon Communications pfSense	[OOTB] pfSense Syslog	Syslog	Предназначен для обработки событий, поступающих от межсетевого экрана pfSense, поступающих по Syslog.
Rubicon Communications pfSense	[OOTB] pfSense w/o hostname	Syslog	Предназначен для обработки событий, поступающих от межсетевого экрана pfSense. Syslog-заголовок этих событий не содержит имени хоста.
RuPost LLC WorksPad	[OOTB] RuPost LLC WorksPad CEF syslog	Syslog	Предназначен для обработки части событий системы RuPost LLC WorksPad (версия 6.3.70) в формате CEF, поступающих по Syslog.
SafeTech CA SQL	[OOTB] SafeTech CA SQL	sql	Предназначен для обработки событий, поступающих из СУБД PostgreSQL системы SafeTech CA версии 3.2.
SailPoint IdentityIQ	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
SaltStack	[OOTB] SaltStack syslog	Syslog	Предназначен для обработки однострочных событий, поступающих от системы SaltStack (версия 3004.1 и старше) по Syslog. Нормализатор не поддерживает обработку многострочных событий.
SecurityCode Continent 3.9	[OOTB] SecurityCode Continent 3.9 json	json	Предназначен для обработки событий системы SecurityCode Continent версии 3.9.2, поступающих от утилиты kuma-kont в формате json.
SecurityCode Continent 4	[OOTB] SecurityCode Continent 4 syslog	regexp	Предназначен для обработки событий системы SecurityCode Continent версии 4, поступающих по Syslog.
Sendmail	[OOTB] Sendmail syslog	Syslog	Предназначен для обработки событий Sendmail версии 8.15.2, поступающих по Syslog.

Название системы	Название нормализатора	Тип	Описание нормализатора
SentinelOne	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Seqrite EPS	[OOTB] Seqrite EPS CEF	cef	Предназначен для обработки событий, поступающих от системы Seqrite EPS версии 6.0 в формате CEF.
Skype for Business	[OOTB] Microsoft Products for KUMA 3 [OOTB] Microsoft Products via KES WIN NG for KUMA 3.2 [OOTB] Microsoft Products via KES WIN NG for KUMA 4.0.1	xml	Предназначен для обработки части событий из журнала системы Skype for Business, журнал Lync Server.
Snort	[OOTB] Snort 3 json file	json	Предназначен для обработки событий Snort версии 3 в формате JSON.
Sophos Central	[OOTB] Sophos Central syslog	Syslog	Предназначен для обработки части событий, поступающих от системы Sophos Central версии 1.2 по Syslog в формате CEF от интеграционного скрипта Sophos-Central-SIEM-Integration.
Sonicwall TZ	[OOTB] Sonicwall TZ Firewall syslog	Syslog	Предназначен для обработки событий, поступающих от межсетевого экрана Sonicwall TZ в формате key-value (версия 7.3), в формате CEF (версия 6.5, 7.3) по Syslog.
Solar webProxy	[OOTB] Solar WebProxy syslog	regexp	Предназначен для обработки событий, поступающих от Solar webProxy версии 4.2 в формате siem-log по Syslog.
SolarWinds DameWare MRC	[OOTB] SolarWinds DameWare MRC xml	xml	Предназначен для обработки части событий системы DameWare Mini Remote Control (MRC) версия 7.5, хранящихся в журнале Application операционной системы Windows. Нормализатор обрабатывает события, создаваемые провайдером dwmrcs.
SolarWinds SFTP & SCP Server file	[OOTB] SolarWinds SFTP & SCP Server file	regexp	Предназначен для обработки журнала событий SolarWinds SFTP & SCP Server (версия 2.2), хранящегося в файле SftpServer.log.
Sophos Firewall	[OOTB] Sophos Firewall syslog	regexp	Предназначен для обработки событий, поступающих от Sophos Firewall версии 20 по Syslog.
Sophos XG	[OOTB] Sophos XG	regexp	Предназначен для обработки событий от межсетевого экрана Sophos XG.
Squid	[OOTB] Squid access Syslog	Syslog	Предназначен для обработки событий прокси-сервера Squid, поступающих по протоколу Syslog.
Squid	[OOTB] Squid access.log file	regexp	Предназначен для обработки событий журнала Squid прокси-сервера Squid. Источник событий – журналы access.log
Staffcop Enterprise	[OOTB] Staffcop Enterprise syslog CEF	regexp	Предназначен для обработки событий, поступающих от Staffcop Enterprise версии 5.4, 5.5 в формате CEF по Syslog.
S-Terra VPN Gate	[OOTB] S-Terra	Syslog	Предназначен для обработки событий от устройств S-Terra VPN Gate.
Stormshield firewall	[OOTB] Stormshield firewall syslog	Syslog	Предназначен для обработки событий, поступающих от системы Stormshield firewall версии 4.8 и 5.0 в формате key-value по протоколу Syslog.
Suricata	[OOTB] Suricata json file	json	Предназначен для обработки событий Suricata версии 7.0.1, хранящихся в файле в формате JSON. Нормализатор поддерживает обработку следующих типов событий: flow, anomaly, alert, dns, http, ssl, tls, ftp, ftp_data, ftp, smb, rdp, pgsql, modbus, quic, dhcp, bittorrent_dht, rfb.
Synesis The Wall WAF	[OOTB] Synesis The Wall WAF syslog	Syslog	Предназначен для обработки событий Synesis TheWall WAF, поступающих по Syslog.
TeamPass	[OOTB] TeamPass SQL	sql	Предназначен для обработки событий, поступающих от системы TeamPass (версия 3.1), хранящихся в базе данных.

Название системы	Название нормализатора	Тип	Описание нормализатора
ThreatConnect Threat Intelligence Platform	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
ThreatQuotient	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Tionix Cloud Platform	[OOTB] Tionix Cloud Platform syslog	Syslog	Предназначен для обработки событий системы Tionix Cloud Platform версии 2.9, поступающих по Syslog. Нормализатор осуществляет выборку части данных из событий.
Tionix VDI	[OOTB] Tionix VDI file	regexp	Предназначен для обработки части событий системы Tionix VDI (версия 2.8), хранящихся в файле tionix_Intmov.log.
TrapX DeceptionGrid	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Trend Micro Control Manager	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Trend Micro Deep Security	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Trend Micro NGFW	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Trustwave Application Security DbProtect	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Umbraco CMS	[OOTB] Umbraco CMS syslog	regexp	Предназначен для обработки событий системы Umbraco CMS версии 11.4.1 в формате Syslog.
Unbound	[OOTB] Unbound Syslog	Syslog	Предназначен для обработки событий, поступающих по Syslog от DNS-сервера Unbound.
UserGate	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF, поступающих от системы UserGate по Syslog.
Varonis DatAdvantage	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Veeam Software – Veeam Backup & Replication	[OOTB] Veeam Software Veeam Backup & Replication syslog	regexp	Предназначен для обработки событий, поступающих от системы Veeam Software – Veeam Backup & Replication версии 12.1 по Syslog.
Veriato 360	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
ViPNet TIAS	[OOTB] Vipnet TIAS syslog	Syslog	Предназначен для обработки событий системы ViPNet TIAS версии 3.8, поступающих по Syslog.
VK Private Cloud	[OOTB] VK Private Cloud syslog	regexp	Предназначен для обработки событий аудита VK Private Cloud (версия 1.0), поступающих по Syslog.
VK WorkSpace Mail	[OOTB] VK WorkSpace Mail syslog	Syslog	Предназначен для обработки событий, поступающих от системы VK WorkSpace Mail версии 1.23 по Syslog в формате key-value.
VMware ESXi	[OOTB] VMware ESXi syslog	regexp	Предназначен для обработки событий VMware ESXi (поддержка ограниченного количества событий от ESXi с версиями 5.5, 6.0, 6.5, 7.0), поступающих по Syslog.
VMWare Horizon	[OOTB] VMWare Horizon - Syslog	Syslog	Предназначен для обработки событий, поступающих от системы VMWare Horizon версии 2106 по Syslog.
VMwareCarbon Black EDR	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Vmware Vcenter	[OOTB] VMware Vcenter API	xml	Предназначен для обработки событий VMware Vcenter версии 7, получаемых по API.
Vormetric Data Security Manager	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.

Название системы	Название нормализатора	Тип	Описание нормализатора
Votiro Disarmer for Windows	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Vsftpd	[OOTB] Vsftpd syslog	regexp	Предназначен для обработки событий, поступающих от системы Vsftpd версии 3.0.5 по Syslog.
Wallix AdminBastion	[OOTB] Wallix AdminBastion syslog	regexp	Предназначен для событий, поступающих от системы Wallix AdminBastion по Syslog.
WatchGuard - Firebox	[OOTB] WatchGuard Firebox syslog	Syslog	Предназначен для обработки событий межсетевых экранов WatchGuard Firebox (версия OS v2026.1.B730198), поступающих по Syslog.
Webmonitorx	[OOTB] Webmonitorx json	regexp	Предназначен для обработки событий, поступающих от системы Webmonitorx в формате JSON.
Webroot BrightCloud	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Windchill FRACAS	[OOTB] PTC Winchill Fracas	regexp	Предназначен для обработки событий системы регистрации сбоев Windchill FRACAS.
Yandex Cloud	[OOTB] Yandex Cloud	regexp	Предназначен для обработки части событий аудита системы Yandex Cloud. Нормализатор поддерживает обработку событий аудитного журнала уровня конфигурации: IAM (Yandex Identity and Access Management), Compute (Yandex Compute Cloud), Network (Yandex Virtual Private Cloud), Storage (Yandex Object Storage), Resourcemanager (Yandex Resource Manager), Backup.
Zabbix	[OOTB] Zabbix SQL	sql	Предназначен для обработки событий Zabbix версии 6.4.
Zecurion DLP	[OOTB] Zecurion DLP syslog	regexp	Предназначен для обработки части событий системы Zecurion DLP версии 13.0, поступающих в формате CEF по Syslog.
ZEEK IDS	[OOTB] ZEEK IDS json file	json	Предназначен для обработки журналов системы ZEEK IDS в формате JSON. Нормализатор поддерживает события от ZEEK IDS версии 1.8.
Zettaset BDEncrypt	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
Zscaler Nanolog Streaming Service (NSS)	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF.
АйТи Бастион – Синоникс	[OOTB] Bastion Synonyx CEF	regexp	Предназначен для обработки событий в формате CEF, поступающих от системы АйТи Бастион – Синоникс версии 1.7.
АйТи Бастион – СКДПУ	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF, поступающих от системы АйТи Бастион – СКДПУ по Syslog.
А-реал Интернет Контроль Сервер (ИКС)	[OOTB] A-real IKS syslog	regexp	Предназначен для обработки событий системы А-реал Интернет Контроль Сервер (ИКС), поступающих по Syslog. Нормализатор поддерживает события от A-real IKS версии 7.0 и выше.
Бизнес Решения – Compass	[OOTB] Biznes Resheniya Compass	regexp	Предназначен для обработки типов событий аудита системы Бизнес Решения – Compass версии 6.7.7 и 6.7.8, поступающих из Kafka.
Веб-сервер Angie	[OOTB] Angie syslog	Syslog	Предназначен для обработки событий, поступающих от системы Angie и Angie Pro (версия 1.10.1) по Syslog.
Веб-сервер Apache	[OOTB] Apache HTTP Server file	regexp	Предназначен для обработки событий Apache HTTP Server версии 2.4, хранящихся в файле. Нормализатор поддерживает обработку событий журнала Application в форматах Common или Combined Log, и журнала Error. Ожидаемый формат журнала Error: `[%t] [%-m:%l] [pid %P:tid %T] [server\ %v] [client\ %a] %E: %M;\ referer\ %-{Referer}i`
Веб-сервер Apache	[OOTB] Apache HTTP Server syslog	Syslog	Предназначен для обработки событий системы Apache HTTP Server, поступающих по Syslog. Нормализатор поддерживает обработку событий Apache HTTP Server версии 2.4 журнала Access в формате Common или Combined Log, и журнала Error. Ожидаемый формат событий журнала Error: `[%t] [%-m:%l] [pid %P:tid %T] [server\ %v] [client\ %a] %E: %M;\ referer\ %-{Referer}i`

Название системы	Название нормализатора	Тип	Описание нормализатора
Веб-сервер Lighttpd	[OOTB] Lighttpd syslog	Syslog	Предназначен для обработки событий Access системы Lighttpd, поступающих по Syslog. Нормализатор поддерживает обработку событий Lighttpd версии 1.4. Ожидаемый формат событий журнала Access: `$remote_addr $http_request_host_name $remote_user [$time_local] "$request" $status $body_bytes_sent "$http_referer" "$http_user_agent"`
ИВК Кольчуга-К	[OOTB] Kolchuga-K Syslog	Syslog	Предназначен для обработки событий, поступающих от системы ИВК Кольчуга-К, версии ЛКНВ.466217.002 по Syslog.
ИнфоТеКС ViPNet IDS	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF, поступающих от системы ИнфоТеКС ViPNet IDS по Syslog.
ИнфоТеКС ViPNet Coordinator	[OOTB] VipNet Coordinator Syslog [OOTB] VipNet Coordinator CEF	Syslog	Нормализатор [OOTB] VipNet Coordinator Syslog предназначен для обработки событий от системы ИнфоТеКС ViPNet Coordinator, поступающих по Syslog. Нормализатор [OOTB] VipNet Coordinator CEF предназначен для обработки событий, поступающих от системы ИнфоТеКС ViPNet Coordinator (версии 4.5) в формате CEF.
Код безопасности - Континент	[OOTB][regexp] Continent IPS/IDS & TLS	regexp	Предназначен для обработки журнала событий устройств Континент IPS/IDS.
Код безопасности - Континент	[OOTB] Continent SQL	sql	Предназначен для получения событий системы Континент из базы данных.
Код Безопасности SecretNet 7	[OOTB] SecretNet SQL	sql	Предназначен для обработки событий, полученных коннектором из базы данных системы SecretNet.
Конфидент - Единый центр управления Dallas Lock	[OOTB] Confident Dallas Lock syslog CEF	regexp	Предназначен для обработки событий, поступающих от систем: Dallas Lock 8 (версия 11.4.2.843, 12.10.6.877), Единый центр управления (ЕЦУ) Dallas Lock (версия 4.0.294.0, 4.0.354.0) в формате CEF.
Конфидент - Dallas Lock	[OOTB] Confident Dallas Lock syslog CEF	regexp	Предназначен для обработки событий, поступающих от системы Dallas Lock 8 (версия 11.4.2) в формате CEF.
КриптоПро NGate	[OOTB] Ngate Syslog	Syslog	Предназначен для обработки событий, поступающих от системы КриптоПро NGate по Syslog.
Маршрутизаторы H3C (Huawei-3Com)	[OOTB] H3C Routers syslog	regexp	Предназначен для обработки типов событий, поступающих от сетевых устройств H3C (Huawei-3Com) SR6600 (прошивка Comware 7) по Syslog. Нормализатор поддерживает формат событий standard (RFC 3164-compliant format).
НТ Мониторинг и аналитика	[OOTB] Syslog-CEF	Syslog	Предназначен для обработки событий в формате CEF, поступающих от системы НТ Мониторинг и аналитика по Syslog.
Прокси-сервер BlueCoat	[OOTB] BlueCoat Proxy v0.2	regexp	Предназначен для обработки событий прокси-сервера BlueCoat. Источник событий – журнал событий прокси-сервера BlueCoat.
СКДПУ НТ Шлюз доступа	[OOTB] Bastion SKDPU-GW syslog	Syslog	Нормализатор для обработки событий системы СКДПУ НТ Шлюз доступа версии 7.0 (сборка17, обновление 14) и 7.1.1, поступающих по Syslog.
Солар Дозор	[OOTB] Solar Dozor Syslog	Syslog	Предназначен для обработки событий, поступающих от системы Солар Дозор версии 7.9 по Syslog. Нормализатор поддерживает обработку событий в пользовательском формате и не поддерживает обработку событий в формате CEF.
Яндекс 360	[OOTB] Yandex 360 json	json	Предназначен для обработки событий, поступающих от системы Яндекс 360 в формате JSON.
Яндекс Браузер корпоративный	[OOTB] Yandex Browser	json	Предназначен для обработки событий, поступающих от корпоративной версии Яндекс Браузера версии 23, 24.4, 25.2.
-	[OOTB] Syslog header	Syslog	Предназначен для обработки событий, поступающих по Syslog. Нормализатор выполняет парсинг Syslog-заголовка события, поле message события не затрагивается. В случае необходимости вы можете выполнить парсинг поля message другими нормализаторами.

Создание коллектора

Облачные коллекторы не поддерживают передачу событий с помощью коннекторов типа **netflow**, **sflow**, **udp**, **snmp-trap**. Коннекторы этих типов поддерживаются в локальных коллекторах.

Вы можете создать коллектор в веб-интерфейсе Kaspersky SIEM Cloud одним из следующих способов:

- В разделе **Мониторинг** → **Ресурсы и сервисы** нажмите **Подключить источник**.
- В разделе **Мониторинг** → **Ресурсы и сервисы** → **Коллекторы** нажмите **Создать**.

Каждый облачный коллектор должен иметь сертификат для проверки подлинности сервиса. В противном случае коллектор не сможет принимать события. Предустановленные коллекторы из типовой конфигурации решения уже имеют сертификаты. Если вы хотите создать дополнительный коллектор и развернуть его в облачной инфраструктуре, вам нужно самостоятельно создать для такого коллектора сертификат. Информация о привязке сертификата к коллектору приведена в инструкции ниже.

Создание коллектора состоит из следующих этапов:

1 Подключение источников событий

1. В разделе **Подключение источников** на вкладке **Основные параметры** заполните следующие поля:

   a. В поле **Название коллектора** введите уникальное имя коллектора. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   При создании некоторых типов коллекторов вместе с ними автоматически создаются агенты, имеющие название `agent: <Название коллектора>, auto created`. Если такой агент уже создавался ранее и не был удален, то коллектор с названием `<Название коллектора>` невозможно будет создать. В этом случае необходимо или указать другое название коллектора, или удалить ранее созданный агент.

   b. В поле **Обработчики** при необходимости укажите количество обработчиков, которые коллектор может запускать одновременно для параллельной обработки событий. Укажите целое положительное число от 0 до 999. Если указано 0, то используется число логических ядер CPU.

   c. В поле **Описание** можно добавить описание коллектора: до 256 символов в кодировке Unicode.

2. На вкладке **Дополнительные параметры** заполните следующие поля:

   a. При необходимости с помощью переключателя **Отладка** включите логирование операций сервиса. Сообщения об ошибках сервиса коллектора помещаются в журнал, даже если режим отладки выключен. Журнал можно просмотреть на машине, где установлен коллектор, в директории `/opt/kaspersky/kuma/collector/<идентификатор коллектора>/log/collector`.

   b. Переключатель **Периодическое создание дампа** используется по запросу Службы технической поддержки для генерации отчетов по потреблению ресурсов (cpu, ram и других) в виде дампов.

   c. В поле **Настройки дампа** вы можете указать параметры создания дампа. Порядок заполнения этого поля уточняйте в Службе технической поддержки.

2 Добавление коннектора

1. В разделе **Транспорт** на вкладке **Основные параметры** в раскрывающемся списке **Коннектор** выберите нужный коннектор или создайте новый, нажав **Создать**.

   Если вы выбрали коннектор из списка, то в разделе **Транспорт** отобразятся параметры выбранного коннектора.

   Если после создания коллектора вы планируете развернуть его в облачной инфраструктуре, коллектор должен иметь сертификат для проверки подлинности сервиса. В противном случае коллектор не сможет принимать события.

   Чтобы привязать сертификат к коллектору:

   a. Сформируйте PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера.

   b. В веб-интерфейсе Kaspersky SIEM Cloud создайте PFX-секрет и загрузите в него PFX-сертификат. Вы также можете создать секрет при создании коннектора или коллектора.

   c. В списке **Коннектор** выберите один из вариантов:

   - Если вы хотите выбрать существующий коннектор, убедитесь, что вы выбираете коннектор, в свойствах которого указан PFX-секрет, содержащий сертификат коллектора. PFX-секрет должен быть выбран в свойствах коннектора на вкладке **Дополнительные параметры,** при выборе значения **Нестандартный PFX** в параметре **Режим TLS**.

   - Если вы хотите создать новый коннектор, перейдите к следующему шагу инструкции. При создании коннектора выберите PFX-секрет, содержащий сертификат коллектора. Это можно сделать на вкладке **Дополнительные параметры,** при выборе значения **Нестандартный PFX** в параметре **Режим TLS**.

2. Если вы нажали **Создать**, раскрывающемся списке **Тип** выберите тип коннектора и укажите его параметры на вкладках **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа коннектора:

   - internal
   - tcp
   - udp (доступно только для локальных коллекторов)
   - netflow (доступно только для локальных коллекторов)
   - sflow (доступно только для локальных коллекторов)
   - nats-jetstream
   - kafka
   - http
   - sql
   - file
   - 1c-log

- 1c-xml
- diode
- ftp
- nfs
- wmi
- wec
- etw
- snmp
- snmp-trap (доступно только для локальных коллекторов)
- kata\edr
- vmware
- elastic
- office365
- dfi
- universalAPI
- smb

При использовании типа коннектора **tcp** или **udp** на этапе добавления нормализатора в поле событий `DeviceAddress`, если оно пустое, будут записаны IP-адреса устройств, с которых были получены события.

При использовании типа коннектора **wmi**, **wec** или **etw** будут автоматически созданы агенты для приема событий Windows.

Рекомендуется использовать кодировку по умолчанию (то есть UTF-8) и применять другие параметры только при получении в полях событий битых символов.

Для настройки коллекторов Kaspersky SIEM Cloud на прослушивание портов с номерами меньше `1000` сервис нужного коллектора необходимо запускать с правами root. Для этого после установки коллектора в его конфигурационный файл `systemd` в раздел `[Service]` требуется добавить строку:

```
AmbientCapabilities=CAP_NET_BIND_SERVICE
```

Systemd-файл располагается в директории `/usr/lib/systemd/system/kuma-collector-<идентификатор коллектора>.service`.

Коннектор добавлен в набор ресурсов коллектора. Созданный коннектор доступен только в этом наборе ресурсов и не отображается в разделе веб-интерфейса **Мониторинг** → **Ресурсы и сервисы** → **Коннекторы**.

❸ Добавление нормализатора

1. В разделе **Парсинг событий** на вкладке **Схема парсинга** нажмите на кнопку **+ Добавить парсинг событий**.

2. Если вы хотите создать нормализатор в виде отдельного ресурса, установите флажок **Сохранить нормализатор**. Если флажок установлен, нормализатор будет доступен для выбора в других коллекторах. По умолчанию флажок снят.

3. В поле **Название** введите уникальное имя нормализатора. Максимальная длина имени: до 128 символов в кодировке Unicode.

   a. В раскрывающемся списке **Метод парсинга** выберите тип получаемых событий. В зависимости от выбранного значения вы можете использовать преднастроенные правила сопоставления полей событий или указать правила вручную. При выборе определенных методов парсинга могут стать доступны дополнительные параметры, для которых вам нужно указать значения.

   Доступные методы парсинга:

   json

   Этот метод парсинга используется для обработки данных в формате JSON, в которых каждый объект, включая его вложенные объекты, занимает одну строку файла.

   При обработке файлов с иерархически выстроенными данными вы можете обращаться к полям вложенных объектов, указывая названия параметров поочередно через точку. Например, к параметру `username` из строки `"user":{"username":"system:node:example-01"}` можно обратиться с помощью запроса `user.username`.

   Файлы обрабатываются построчно. Многострочные объекты с вложенными структурами могут быть нормализованы неправильно.

   В сложных схемах нормализации, где используются дополнительные нормализаторы, все вложенные объекты обрабатываются на первом уровне нормализации за исключением случаев, когда условия дополнительной нормализации не заданы и обрабатываемое событие целиком передается в дополнительный нормализатор.

   В качестве разделителя строк вы можете использовать символы `\n` и `\r\n`. Строки должны быть в кодировке UTF-8.

   Если вы хотите передавать сырое событие для дополнительной нормализации, на каждом уровне вложенности в окне **Дополнительный парсинг события** в раскрывающемся списке **Использовать сырое событие** выберите **Да**.

   cef

   Этот метод парсинга используется для обработки данных в формате CEF.

   При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат Kaspersky SIEM Cloud, нажав на кнопку **Применить сопоставление по умолчанию**.

   regexp

   Этот метод парсинга используется для создания собственных правил обработки данных в формате с использованием регулярных выражений.

Вам нужно добавить регулярное выражение (синтаксис RE2) с именованными группами захвата в поле блока параметров **Нормализация**. Имя группы захвата и ее значение будут считаться полем и значением сырого события, которое можно будет преобразовать в поле события формата Kaspersky SIEM Cloud.

Чтобы добавить правила обработки событий:

1. При необходимости в поле **Примеры событий** скопируйте пример данных, которые вы хотите обработать. Мы рекомендуем выполнить этот шаг.

   Вы также можете сгенерировать регулярные выражения на основе добавленных примеров по кнопке **Сгенерировать регулярное выражение с помощью KIRA**. В этом случае сгенерированные регулярные выражения автоматически добавятся в блок параметров **Нормализация**.

2. В поле блока параметров **Нормализация** добавьте регулярное выражение с именованными группами захвата в синтаксисе RE2, например `"(?P<name>regexp)"`. Регулярное выражение, добавленное в поле блока параметров **Нормализация**, должно полностью совпадать с событием. При разработке регулярного выражения рекомендуется использовать специальные символы, обозначающие начало и конец текста: `^`, `$`.

   Вы можете добавить несколько регулярных выражений или удалить регулярные выражения. Для добавления регулярного выражения нажмите на кнопку **Добавить регулярное выражение**. Для удаления регулярного выражения нажмите рядом с ним на значок удаления ✕.

3. Нажмите на кнопку **Перенести названия полей в таблицу**.

   Имена групп захвата отображаются в столбце **Поле KUMA** таблицы **Сопоставление**. Вы можете выбрать соответствующее группе захвата поле Kaspersky SIEM Cloud в столбце напротив каждой группы захвата. Если вы именовали группы захвата в соответствии с форматом CEF, вы можете использовать автоматическое сопоставление CEF, установив флажок **Использовать синтаксис CEF при нормализации**.

Правила обработки событий будут добавлены.

syslog

Этот метод парсинга используется для обработки данных в формате syslog.

При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат Kaspersky SIEM Cloud, нажав на кнопку **Применить сопоставление по умолчанию**.

Для парсинга событий в формате rfc5424 с секцией `structured-data` вам нужно в раскрывающемся списке **Сохранить дополнительные поля** выбрать **Да**. В этом случае значения из секции `structured-data` станут доступны в полях `Extra`.

csv

Этот метод парсинга используется для создания собственных правил обработки данных в формате CSV.

При выборе этого метода парсинга вам нужно в поле **Разделитель** указать разделитель значений в строке. В качестве разделителя значений в строке можно использовать любой однобайтовый символ ASCII.

kv

Этот метод парсинга используется для обработки данных в формате ключ-значение. Доступные параметры метода парсинга описаны в таблице ниже.

Доступные параметры метода парсинга

Параметр	Описание
Разделитель пар	Символ для разделения пар ключ-значение. Вы можете указать любое односимвольное (1 байт) значение. Указанное значение не должно совпадать со значением, указанным в поле **Разделитель значений**.
Разделитель значений	Символ для разделения ключа и значения. Вы можете указать любое односимвольное (1 байт) значение. Указанное значение не должно совпадать со значением, указанным в поле **Разделитель пар**.

xml

Этот метод парсинга используется для обработки данных в формате XML, в которых каждый объект, включая вложенные объекты, занимает одну строку файла. Файлы обрабатываются построчно.

Если вы хотите передавать сырое событие для дополнительной нормализации, на каждом уровне вложенности в окне **Дополнительный парсинг события** в раскрывающемся списке **Использовать сырое событие** выберите **Да**.

При выборе этого метода парсинга вы можете указать ключевые атрибуты XML, которые требуется извлекать из тегов, в блоке параметров **Атрибуты XML**. Если в структуре XML в одном теге есть атрибуты XML с разными значениями, вы можете определить значение, указав ключ к значению в столбце **Исходные данные** таблицы **Сопоставление**.

Чтобы добавить ключевые атрибуты XML:

1. Нажмите на кнопку **+ Добавить поле**.
2. В открывшемся окне укажите путь к атрибуту XML.

Вы можете добавить несколько атрибутов XML и удалить атрибуты XML. Для удаления отдельного атрибута XML нажмите рядом с ним на значок удаления ✕. Для удаления всех атрибутов XML нажмите на кнопку **Сбросить**.

Если ключевые атрибуты XML не указаны, при сопоставлении полей уникальный путь к значению XML будет представлен последовательностью тегов.

Нумерация тегов

В Kaspersky SIEM Cloud доступна автоматическая нумерация тегов в событиях в формате XML. Это позволяет распарсить событие с одинаковыми тегами или неименованными тегами, такими как `<Data>`.

В качестве примера мы используем нумерацию тегов атрибута `EventData` события Microsoft Windows PowerShell event ID 800.

Посмотреть события Microsoft Windows PowerShell event ID 800

```
<Event xmlns="http://schemas .microsoft.com/win/2004/08/events/event">
        <System>
                <Provider Name="Microsoft-Windows-ActiveDirectory_DomainService" Guid="{0e8478c5-3605-4e8c-
8497-1e730c959516}" EventSourceName="NTDS" />
                <EventID Qualifiers="0000">0000</EventID>
                <Version>@</Version>
                <Level>4</Level>
                <Task>15</Task>
                <Opcode>0</Opcode>
                <Keywords >0x8080000000000000</Keywords>
                <TimeCreated SystemTime="2000-01-01T00:00:00.659495900Z" />
                <EventRecordID>55647</EventRecordID>
                <Correlation />
                <Execution ProcessID="1" ThreadID="1" />
                <Channel>service</Channel>
```

```
                <Computer>computer</Computer>
                <Security UserID="0000" />
        </System>
        <EventData>
                <Data>583</Data>
                <Data>36</Data>
                <Data>192.168.0.1:5084</Data>
                <Data>level</Data>
                <Data>name, lDAPDisplayName</Data>
                <Data />
                <Data>5545</Data>
                <Data>3</Data>
                <Data>0</Data>
                <Data>0</Data>
                <Data>0</Data>
                <Data>15</Data>
                <Data>none</Data>
        </EventData>
</Event>
```

Для парсинга событий с одинаковыми тегами или неименованными тегами вам нужно настроить нумерацию тегов и маппинг данных для пронумерованных тегов с полями события Kaspersky SIEM Cloud.

Kaspersky SIEM Cloud поддерживает одновременное использование атрибутов XML и нумерации тегов в рамках одного экстранормализатора. Если атрибут XML содержит неименованные теги или одинаковые теги, мы рекомендуем использовать нумерацию тегов. Если атрибут XML содержит только именованные теги, мы рекомендуем использовать атрибуты XML.

Для использования атрибутов XML и нумерации тегов в экстранормализаторах вам нужно последовательно включить параметр **Использовать сырое событие** в каждом экстранормализаторе по пути следования события в целевой экстранормализатор и в целевом экстранормализаторе.

В качестве примера работы нумерации тегов вы можете обратиться к нормализатору **MicrosoftProducts**. Параметр **Использовать сырое событие** включен последовательно в экстранормализаторах **AD FS** и **424**.

Чтобы настроить парсинг событий с неименованными или одинаковыми тегами:

1. Откройте существующий или создайте новый нормализатор.

2. В окне нормализатора **Основной парсинг событий** в раскрывающемся списке **Метод парсинга** выберите **xml**.

3. В поле **Нумерация тегов** нажмите на кнопку **+ Добавить поле**.

4. В отобразившемся поле укажите полный путь к тегу, элементам которого требуется присвоить порядковый номер, например `Event.EventData.Data`. Первому тегу будет присвоен номер 0. Если тег пустой, например `<Data />`, ему также будет присвоен порядковый номер.

5. Для настройки маппинга данных в группе параметров **Сопоставление** нажмите на кнопку **+ Добавить строку** и выполните следующие действия:

   a. В отобразившейся строке в поле **Исходные данные** укажите полный путь к тегу и индекс тега. Например, для события Microsoft Windows PowerShell event ID 800 из примера выше полные пути к тегам и индексы тегов будут выглядеть следующим образом:

      - `Event.EventData.Data.0`
      - `Event.EventData.Data.1`
      - `Event.EventData.Data.2`

   b. В раскрывающемся списке **Поле KUMA** выберите поле в событии Kaspersky SIEM Cloud, в которое попадет значение из пронумерованного тега после выполнения парсинга.

6. Сохраните изменения одним из следующих способов:

   - Если вы создали новый нормализатор, нажмите на кнопку **Сохранить**.
   - Если вы изменили существующий нормализатор, в коллекторе, к которому привязан нормализатор, нажмите на кнопку **Обновить параметры**.

Настройка парсинга будет завершена.

netflow

Этот метод парсинга используется для обработки данных во всех поддерживаемых форматах на основе протокола NetFlow: NetFlow v5, NetFlow v9 и IPFIX.

При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат Kaspersky SIEM Cloud, нажав на кнопку **Применить сопоставление по умолчанию**. При этом будут учтены исходные поля всех версий NetFlow (NetFlow v5, NetFlow v9 и IPFIX).

Если метод парсинга **netflow** выбран для основного парсинга, дополнительная нормализация недоступна.

> В правилах сопоставления по умолчанию для метода парсинга **netflow** в полях событий Kaspersky SIEM Cloud не указывается тип протокола. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** вам нужно создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

netflow5

Этот метод парсинга используется для обработки данных в формате NetFlow v5.

При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат Kaspersky SIEM Cloud, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **netflow5** выбран для основного парсинга, дополнительная нормализация недоступна.

В правилах сопоставления по умолчанию для метода парсинга **netflow5** в полях событий Kaspersky SIEM Cloud не указывается тип протокола. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** вам нужно создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

netflow9

Этот метод парсинга используется для обработки данных в формате NetFlow v9.

При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат Kaspersky SIEM Cloud, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **netflow9** выбран для основного парсинга, дополнительная нормализация недоступна.

В правилах сопоставления по умолчанию для метода парсинга **netflow9** в полях событий Kaspersky SIEM Cloud не указывается тип протокола. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** вам нужно создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

sflow5

Этот метод парсинга используется для обработки данных в формате sflow5.

При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат Kaspersky SIEM Cloud, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **sflow5** выбран для основного парсинга, дополнительная нормализация недоступна.

ipfix

Этот метод парсинга используется для обработки данных в формате IPFIX.

При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат Kaspersky SIEM Cloud, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **ipfix** выбран для основного парсинга, дополнительная нормализация недоступна.

В правилах сопоставления по умолчанию для метода парсинга **ipfix** в полях событий Kaspersky SIEM Cloud не указывается тип протокола. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** вам нужно создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

sql

Нормализатор использует этот метод парсинга для обработки данных, полученных с помощью выборки из базы данных.

Этот метод парсинга становится доступным, только если в разделе Транспорт вы добавили коннектор с типом sql.

normalizer

Этот метод парсинга позволяет переиспользовать ранее созданный нормализатор в качестве основного или дополнительного для обработки событий.

При выборе этого метода парсинга вам нужно в раскрывающемся списке **Нормализатор** выбрать один из ранее созданных нормализаторов с типом json, cef, regexp, syslog, csv, kv, xml или sql. Нормализаторы с методом парсинга **normalizer** недоступны для выбора.

b. В раскрывающемся списке **Сохранить исходное событие** выберите, требуется ли сохранять исходное сырое событие в повторно созданном нормализованном событии:

- **Не сохранять** – не сохранять исходное событие. Это значение выбрано по умолчанию.
- **При возникновении ошибок** – сохранять исходное событие в поле `Raw` нормализованного события, если в процессе парсинга возникли ошибки. Вы можете использовать это значение при отладке сервиса. В этом случае появление у событий непустого поля `Raw` будет являться признаком неполадок.
- **Всегда** – сохранять сырое событие в поле `Raw` нормализованного события.

c. В раскрывающемся списке **Сохранить дополнительные поля** выберите, требуется ли сохранять поля исходного события в нормализованном событии, если для них не было настроено сопоставление:

Это поле недоступно, если в поле **Метод парсинга** выбрано значение **normalizer**.

- **Нет**. Это значение выбрано по умолчанию.
- **Да**. Поля исходного события сохраняются в поле `Extra` нормализованного события.

d. При необходимости в поле **Примеры событий** укажите пример данных, которые вы хотите обработать. Мы рекомендуем выполнить этот шаг.

Это поле недоступно, если в поле **Метод парсинга** выбрано значение **normalizer**.

Вы можете добавить несколько примеров событий. Каждый новый пример нужно указывать с новой строки. При этом в таблице **Сопоставление** его результат парсинга отобразится в столбце **Примеры**. Это позволяет проверить правильность сопоставления полей для разных типов входящих событий.

Ограничения при парсинге примеров событий

При парсинге примеров данных, указанных в поле **Примеры событий**, в дополнительном нормализаторе не учитываются следующие параметры:

- обогащение, настроенное в корневом нормализаторе;
- фильтры, заданные в дополнительном нормализаторе;
- значение параметра **Использовать сырое событие**;
- преобразования в корневом нормализаторе;
- преобразования для значения параметра **Поле, которое следует передать в нормализатор**.

4. В блоке параметров **Сопоставление** настройте сопоставление полей исходного события с полями событий Kaspersky SIEM Cloud:

   a. Нажмите на кнопку **+ Добавить строку**.

      Вы можете добавить несколько строк таблицы или удалить строки таблицы. Для удаления строки таблицы установите рядом с ней флажок и нажмите на кнопку **Удалить**.

   b. В столбце **Исходные данные** укажите название поля исходного события, которое вы хотите сопоставить с полем события Kaspersky SIEM Cloud.

      Подробнее о формате названий полей см. в статье Модель данных нормализованного события. Описание сопоставления см. в статье Сопоставление полей предустановленных нормализаторов.

      Если вы хотите создать правила изменения полей исходного события перед записью в поля событий Kaspersky SIEM Cloud, нажмите на значок настройки (⚙) рядом с названием поля и в открывшемся окне **Преобразование** нажмите на кнопку **+ Добавить преобразование**. Вы можете изменить порядок правил и удалить правила. Для изменения порядка правил используйте значки изменения порядка (⋮⋮). Для удаления правила нажмите рядом с ним на значок удаления (✕).

      Доступные преобразования

      Преобразования – это изменения, которые применяются к значению перед записью в поле события.

      Вы можете выбрать в раскрывающемся списке один из следующих типов преобразования:

      - **entropy** – используется для преобразования значения исходного поля с помощью функции вычисления информационной энтропии и помещения результата преобразования в целевое поле типа `float`. Результатом преобразования будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например, когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.

      - **lower** – используется для перевода всех символов значения в нижний регистр.

      - **upper** – используется для перевода всех символов значения в верхний регистр.

      - **regexp** – используется для преобразования значения с помощью указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.

      - **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.

      - **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

        - **Символы на замену** – последовательность символов, которую требуется заменить.

        - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

      - **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` требуется выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.

- **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

- Конвертация закодированных строк в текст:

  - **decodeHexString** – используется для конвертации HEX-строки в текст.

  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  - **unicodeUnescape** – используется для конвертации Unicode-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.

  Мы не рекомендуем использовать несколько дополнительных нормализаторов для последовательного преобразования одного и того же поля. Результат одного преобразования, выполненного дополнительным нормализатором, не используется как входные данные для следующего. В итоговое событие записывается значение, полученное в дополнительном нормализаторе, который первым выполнил обогащение этого поля.

- Преобразование формата IP-адреса в IPv4:

  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.

  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.

- **hexToDecimal** – используется для преобразования числового значения, представленного в шестнадцатеричной системе счисления, в десятичный формат. Преобразование применяется к строковым или числовым полям, содержащим HEX-значения (включая префикс 0x, если он присутствует), и результат записывается в целевое поле события Kaspersky SIEM Cloud в виде целого числа.

  Результатом преобразования является число в десятичной системе, например исходное значение – 0x00FF, после преобразования – 255.

Если в разделе **Транспорт** вы добавили коннектор с типом file, вы можете передать в поле события Kaspersky SIEM Cloud название обрабатываемого коллектором файла или путь к файлу. Для этого в столбце **Исходные данные** укажите одно из следующих значений:

```
Передать в поле события Kaspersky SIEM Cloud название обрабатываемого коллектором файла
```

```
$kuma_fileSourceName
```

```
Передать в поле события Kaspersky SIEM Cloud путь к обрабатываемому коллектором файлу
```

```
$kuma_fileSourcePath
```

Когда вы используете коннектор с типом **file**, новые переменные в нормализаторе будут работать только с точками назначения с типом internal.

c. В столбце **Поле KUMA** в раскрывающемся списке выберите поле события Kaspersky SIEM Cloud. Вы можете найти поле события Kaspersky SIEM Cloud, введя его названия. Если название поля события Kaspersky SIEM Cloud начинается с `DeviceCustom*` и `Flex*`, при необходимости в поле **Подпись** укажите уникальную пользовательскую метку.

Если вы хотите, чтобы Kaspersky SIEM Cloud могла выполнить обогащение событий данными об активах и данные об активах были доступны в карточке алерта при срабатывании корреляционного правила, в таблице **Сопоставление** вам нужно настроить сопоставление полей для адреса хоста и имени хоста в зависимости от назначения актива. Например, вы можете настроить сопоставление для полей событий Kaspersky SIEM Cloud **SourceAddress** и **SourceHostName**, или **DestinationAddress** и **DestinationHostName**. В результате обогащения в карточке события появится поле события Kaspersky SIEM Cloud **SourceAssetID** или **DestinationAssetID** и ссылка, по которой можно будет перейти в карточку актива. В результате обогащения сведения об активе также будут доступны в карточке алерта.

Если вы загрузили данные в поле **Примеры событий**, в таблице отобразится столбец **Примеры** с примерами значений, переносимых из поля исходного события в поле события Kaspersky SIEM Cloud.

Таблица **Сопоставление** недоступна, если в поле **Метод парсинга** выбрано значение **normalizer**.

5. Если вы хотите добавлять дополнительные данные в созданные нормализованные события, создайте в нормализаторе правила обогащения, выполнив следующие действия:

a. Перейдите на вкладку **Обогащение**.

Вкладка **Обогащение** недоступна, если на вкладке **Схема нормализации** в поле **Метод парсинга** выбрано значение **normalizer**.

b. Нажмите на кнопку + **Добавить обогащение**.

Отобразится блок параметров правила обогащения. Вы можете добавить несколько правил обогащения или удалить правила обогащения. Для удаления правила обогащения нажмите рядом с ним на значок удаления (✕).

c. В раскрывающемся списке **Исходный тип** выберите тип источника обогащения. При выборе определенных типов источника обогащения могут стать доступны дополнительные параметры, для которых вам нужно указать значения.

Доступные типы источников обогащения:

константа

Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "константа"

Параметр	Описание
Константа	Значение, которое требуется добавить в поле события. Максимальная длина значения – до 255 символов в кодировке Unicode. Если оставить поле пустым, существующее значение поля события будет удалено.
Целевое поле	Поле события, в которое требуется поместить данные.

Если вы используете функции обогащения событий для полей расширенной схемы с типом `Строка`, `Число` или `Число с плавающей точкой` с помощью константы, в поле будет добавлена константа.

Если вы используете функции обогащения событий для полей расширенной схемы с типом `Массив строк`, `Массив чисел` или `Массив чисел с плавающей точкой` с помощью константы, константа будет добавлена к элементам массива.

словарь

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "словарь"

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.

Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **словарь**, а в параметре **Ключевые поля обогащения** указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку в соответствии с правилами сериализации одного значения в формате TSV.

Пример. В параметре **Ключевые поля обогащения** используется поле расширенной схемы `SA.StringArrayOne`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`. В качестве ключа в словарь будут переданы значения `['a','b','c']`.

Если в параметре **Ключевые поля обогащения** используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом `|`.

Пример. В параметре **Ключевые поля обогащения** используется поле расширенной схемы `SA.StringArrayOne` и строковое поле `Code`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`, а строковое поле `Code` содержит последовательность символов `myCode`. В качестве ключа в словарь будут переданы значения `['a','b','c']|myCode`.

таблица

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "таблица"

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.

Параметр	Описание
Сопоставление	Поля событий для передачи данных: • **Поле словаря** – поля словаря, из которых будут передаваться данные. Доступные поля зависят от выбранного ресурса словаря. • **Поле KUMA** – поля событий, в которые будут передаваться данные. Для выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** вы можете задать название для помещаемых данных.

Первое поле в таблице (**Поле словаря**) считается ключом, с которым будут сопоставляться поля, выбранные из события в качестве ключевых (**Поле KUMA**). В качестве ключа в **Поле словаря** вам нужно выбрать индикатор компрометации, по которому будет осуществляться обогащение, например IP-адрес, URL-адрес или хеш. В правиле необходимо выбрать поле события, соответствующее выбранному индикатору в поле словаря.

Если вы хотите выбрать несколько ключевых полей, вы можете указать их через разделитель `|` (при указании через веб-интерфейс или импорте через CSV-файл), например `<IP-адрес>|<имя пользователя>`.

Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить**. Для удаления строки таблицы нажмите на крестик ✕.

событие

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Доступные параметры типа обогащения описаны в таблице ниже.

Доступные параметры типа обогащения

Параметр	Описание
Целевое поле	Поле события Kaspersky SIEM Cloud, в которое требуется поместить данные.
Исходное поле	Поле события, значение которого будет записано в целевое поле.

Если вы хотите создать правило для изменения исходных данных перед записью в поля событий Kaspersky SIEM Cloud, в блоке параметров **Преобразование** нажмите на кнопку **+ Добавить преобразование**. В раскрывающемся списке **Тип** выберите нужный тип преобразования. Вы можете добавить несколько преобразований по кнопке **+ Добавить преобразование**. Чтобы удалить добавленное преобразование, нажмите рядом с ним на значок корзины.

Доступные преобразования

Преобразования – это изменения, которые применяются к значению перед записью в поле события.

Вы можете выбрать в раскрывающемся списке один из следующих типов преобразования:

- **entropy** – используется для преобразования значения исходного поля с помощью функции вычисления информационной энтропии и помещения результата преобразования в целевое поле типа `float`. Результатом преобразования будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например, когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.

- **lower** – используется для перевода всех символов значения в нижний регистр.

- **upper** – используется для перевода всех символов значения в верхний регистр.

- **regexp** – используется для преобразования значения с помощью указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.

- **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Символы на замену** – последовательность символов, которую требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

- **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` требуется выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.

- **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

- Конвертация закодированных строк в текст:

  - **decodeHexString** – используется для конвертации HEX-строки в текст.

  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  - **unicodeUnescape** – используется для конвертации Unicode-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.

Мы не рекомендуем использовать несколько дополнительных нормализаторов для последовательного преобразования одного и того же поля. Результат одного преобразования, выполненного дополнительным нормализатором, не используется как входные данные для следующего. В итоговое событие записывается значение, полученное в дополнительном нормализаторе, который первым выполнил обогащение этого поля.

- Преобразование формата IP-адреса в IPv4:
  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
- **hexToDecimal** – используется для преобразования числового значения, представленного в шестнадцатеричной системе счисления, в десятичный формат. Преобразование применяется к строковым или числовым полям, содержащим HEX-значения (включая префикс 0x, если он присутствует), и результат записывается в целевое поле события Kaspersky SIEM Cloud в виде целого числа.

  Результатом преобразования является число в десятичной системе, например исходное значение – 0x00FF, после преобразования – 255.

При использовании обогащения событий, у которых в качестве параметра **Тип источника данных** выбрано значение **событие**, а в качестве аргументов используются поля расширенной схемы событий, необходимо учесть следующие особенности:

- Если исходное поле расширенной схемы событий имеет тип `Массив строк`, а целевое поле расширенной схемы событий имеет тип `Строка`, значения будут размещены в целевом поле расширенной схемы событий в формате TSV.

  Пример: в поле расширенной схемы событий `SA.StringArray`, находятся значения `"string1"`, `"string2"`, `"string3"`. Выполняется операция обогащения событий. Результат выполнения операции обогащения событий заносится в поле расширенной схемы событий `DeviceCustomString1`. В поле расширенной схемы событий `DeviceCustomString1` будут находиться значения `["string1", "string2", "string3"]`.

- Если исходное и целевое поля расширенной схемы событий имеют тип `Массив строк`, значения целевого поля расширенной схемы событий будут дополнены значениями исходного поля расширенной схемы событий, а качестве символа-разделителя будет использован символ `","`.

  Пример: в поле расширенной схемы событий `SA.StringArrayOne`, находятся значения `["string1", "string2", "string3"]`, а в поле расширенной схемы событий `SA.StringArrayTwo` находятся значения `["string4", "string5", "string6"]`. Выполняется операция обогащения событий. Результат выполнения операции обогащения событий заносится в поле расширенной схемы событий `SA.StringArrayTwo`. В поле расширенной схемы событий `SA.StringArrayTwo` будут находиться значения `["string4", "string5", "string6", "string1", "string2", "string3"]`.

шаблон

Этот тип обогащения используется, если в поле события нужно записать значение, полученное при обработке шаблонов Go. Мы рекомендуем сопоставлять значение и размер поля. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "шаблон"

Параметр	Описание
Шаблон	Шаблон Go. Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт, например `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.
Целевое поле	Поле события, в которое требуется поместить данные.

Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **шаблон**, целевым полем является поле с типом `Строка`, а исходным полем является поле расширенной схемы событий, содержащее массив строк, то в шаблоне может быть использован один из следующих примеров:

- `{{.SA.StringArrayOne}}`
- ```
  {{- range $index, $element := . SA.StringArrayOne -}}
  {{- if $index}}, {{end}}"{{$element}}"{{- end -}}
  ```

Для преобразования в шаблоне данных поля массива в формат TSV требуется использовать функцию `toString`, например:

```
template {{toString .SA.StringArray}}
```

dns

Этот тип обогащения используется для отправки запросов на DNS-сервер частной сети для преобразования IP-адресов в доменные имена или наоборот. Преобразование IP-адресов в DNS-имена происходит только для частных адресов: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10, fd00::/8.

Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "dns"

Параметр	Описание
URL	URL DNS-сервера, которому вы хотите отправлять запросы. С помощью кнопки **Добавить URL** можно указать несколько URL. Если параметр **URL** не указан, то Kaspersky SIEM Cloud возьмет список DNS-серверов из файла `/etc/resolv.conf`, расположенного на локальном хосте. В этом случае вам нужно включить параметр **Требуется рекурсия**. В противном случае обогащение происходить не будет.
Запросов в секунду	Максимальное количество запросов к DNS-серверу в секунду. Значение по умолчанию: количество vCPU сервера, на котором установлено Ядро Kaspersky SIEM Cloud.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Укажите целое положительное число от 0 до 999. Если указано 0, то используется число логических ядер CPU. Значение по умолчанию: `1`.
Максимальное число событий в очереди обогащения	Максимальное число событий, сохраняемое в очереди для повторной отправки. Значение по умолчанию: `1 000 000`.
Время ожидания	Время ожидания ответа от DNS-сервера (в секундах). Значение по умолчанию: `5`.
Переопределение режима DNS	Используемый метод преобразования: • **Только прямое разрешение DNS** – доменное имя преобразуется в IP-адрес. • **Только обратное разрешение DNS** – IP-адрес преобразуется в доменное имя. • **Прямое и обратное DNS-разрешение** – доменное имя может преобразовываться в IP-адрес и наоборот.
Срок жизни кеша	Время жизни значений (в секундах), хранящихся в кеше. Значение по умолчанию: `60` (сек).
```

Параметр	Описание
Кеш отключен	Параметр, позволяющий включить или выключить кеширование. По умолчанию кеширование включено.
Обновление кэша отключено	Если обновление кеша включено, то по истечении срока жизни кеша коллектор отправляет повторные запросы на DNS-сервер для обновления хранящихся в кеше данных. Этот параметр доступен только при включенном кеше. По умолчанию обновление кеша включено.
Требуется рекурсия	Параметр позволяет включить отправку коллектором рекурсивных запросов к авторитативным DNS-серверам для выполнения обогащения. Значение по умолчанию: **Выключено**.

cybertrace

Для систем с большой нагрузкой на коллектор или коррелятор рекомендуется использовать тип обогащения **cybertrace-http**. Этот тип обогащения возвращает структурированный ответ в формате JSON и корректно различает строки и массивы пользовательских атрибутов, исключая ошибки парсинга.
При обогащении с помощью типа **cybertrace** коллектор получает неструктурированный ответ. Если значение пользовательского атрибута в Kaspersky CyberTrace содержит квадратные скобки, например **[str1**, **str2]**, Kaspersky SIEM Cloud обрабатывает его как массив, а не как строку.

Этот тип обогащения используется для добавления в поля события сведений из потоков данных Kaspersky CyberTrace. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "cybertrace"

Параметр	Описание
URL	URL сервера Kaspersky CyberTrace, которому вы хотите отправлять запросы. Порт Kaspersky CyberTrace по умолчанию: 9999. Обязательный параметр.
Количество подключений	Максимальное количество подключений к серверу Kaspersky CyberTrace, которые может одновременно установить Kaspersky SIEM Cloud. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро Kaspersky SIEM Cloud.
Запросов в секунду	Максимальное количество запросов к серверу в секунду. Значение по умолчанию: `1000`.
Время ожидания	Время ожидания отклика от сервера Kaspersky CyberTrace в секундах. Значение по умолчанию: `30`.
Максимальное кол-во событий в очереди обогащения	Максимальное количество событий, сохраняемое в очереди для переотправки. Значение по умолчанию: `1 000 000`.
Сопоставление	Таблица сопоставления полей событий с типами индикаторов Kaspersky CyberTrace. В столбце **Поле KUMA** указаны названия полей событий, а в столбце **Индикатор CyberTrace** указаны типы индикаторов Kaspersky CyberTrace. Доступные типы индикаторов Kaspersky CyberTrace: • **ip** • **url** • **hash**

В таблице сопоставления требуется указать как минимум одну строку. Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить строку**. Для удаления строки таблицы нажмите на крестик ✕.

cybertrace-http

Этот тип потокового обогащения событий в Kaspersky CyberTrace, который позволяет отправлять большое количество событий одним запросом на API-интерфейс CyberTrace. Мы рекомендуем применять тип обогащения **cybertrace-http** в системах с большим потоком событий. Производительность **cybertrace-http** превосходит показатели типа обогащения **cybertrace**.

Ограничения:

- Тип обогащения **cybertrace-http** невозможно использовать для ретроспективного сканирования в KUMA.
- В случае использования типа обогащения **cybertrace-http** обнаружения киберугроз не сохраняются в истории Kaspersky CyberTrace в окне **Обнаружения**.

Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "cybertrace-http"

Параметр	Описание
Тенант	Тенант, в рамках которого вы планируете работать с Kaspersky CyberTrace. Обязательный параметр.
URL	URL сервера Kaspersky CyberTrace, которому вы хотите отправлять запросы и порт, который использует API CyberTrace. Порт по умолчанию 443. Обязательный параметр.
Секрет	Раскрывающийся список для выбора секрета, в котором хранятся учетные данные для подключения. Обязательный параметр.
Время ожидания	Время ожидания отклика от сервера Kaspersky CyberTrace в секундах. Значение по умолчанию: `30`.
Ключевые поля	Список полей событий, используемых для обогащения событий данными из Kaspersky CyberTrace. Обязательный параметр.
Максимальное кол-во событий в очереди обогащения	Максимальное количество событий, сохраняемое в очереди для переотправки. Значение по умолчанию: `1 000 000`. По достижении 1 млн получаемых событий от сервера Kaspersky CyberTrace события перестают обогащаться, пока число получаемых событий не станет меньше 500 тыс.
Основная версия CyberTrace	Версия Kaspersky CyberTrace. Доступные значения: • **<5** – запросы будут выполняться в тенанте General в Kaspersky CyberTrace и будут использовать новую версию API, соответствующую Kaspersky CyberTrace 5.0 и выше. • **≥ 5.0** – запросы будут использовать версию API, соответствующую Kaspersky CyberTrace 4.x. Значение по умолчанию: **<5**.
Отладка	Параметр, включающий логирование ресурса. По умолчанию переключатель выключен.
Теги	Теги для поиска ресурса.

часовой пояс

Этот тип обогащения используется в коллекторах и коррелляторах, чтобы присвоить событию определенный часовой пояс. Сведения о часовом поясе могут понадобиться при поиске событий, случившихся в нетипичное время, например ночью.

При выборе этого типа обогащения в раскрывающемся списке **Часовой пояс** нужно указать временную зону.

Убедитесь, что выбираемый часовой пояс установлен на сервере сервиса, использующего обогащение. Например, это можно сделать с помощью команды `timedatectl list-timezones`, которая показывает все установленные на сервере часовые пояса. Подробнее об установке часовых поясов смотрите в документации используемой вами операционной системы.

При обогащении события в поле события DeviceTimeZone записывается смещение времени выбранного часового пояса относительно всемирного координированного времени (UTC) в формате `+-чч:мм`. Например, если выбрать временную зону **Asia/Yekaterinburg** в поле `DeviceTimeZone` будет записано значение `+05:00`. Если в обогащаемом событии есть значение поля `DeviceTimeZone`, оно будет перезаписано.

По умолчанию, если в обрабатываемом событии не указан часовой пояс и не настроены правила обогащения по часовому поясу, событию присваивается часовой пояс сервера, на котором установлен сервис (коллектор или коррелятор), обрабатывающий событие. При изменении времени сервера сервис требуется перезапустить.

Допустимые форматы времени при обогащении поля DeviceTimeZone

При обработке в коллекторе поступающих сырых событий следующие форматы времени могут быть автоматически приведены к формату `+-чч:мм` (см. таблицу ниже):

Формат времени в обрабатываемом событии	Пример
+-чч:мм	-07:00
+-ччмм	-0700
+-чч	-07

Если формат даты в поле `DeviceTimeZone` отличается от указанных в таблице, при обогащении события сведениями о часовом поясе в поле записывается часовой пояс серверного времени коллектора. Вы можете создать правила нормализации для нестандартных форматов времени.

геоданные

Этот тип обогащения используется для добавления в поля событий сведений о географическом расположении IP-адресов.

При выборе этого типа в блоке параметров **Сопоставление геоданных с полями события** укажите, из какого поля события будет считан IP-адрес, а также выберите атрибуты геоданных и определите поля событий, в которые геоданные будут записаны:

1. В раскрывающемся списке **Поле события с IP-адресом** выберите поле события, из которого считывается IP-адрес. По этому IP-адресу будет произведен поиск соответствий по загруженным в Kaspersky SIEM Cloud геоданным.

   > При выборе полей события `SourceAddress`, `DestinationAddress` и `DeviceAddress` становится доступна кнопка **Применить сопоставление по умолчанию**. С ее помощью можно добавить преднастроенные пары соответствий атрибутов геоданных и полей события.

2. Для каждого поля события, откуда требуется считать IP-адрес, выберите тип геоданных и поле события, в которое следует записать геоданные.

   - В поле **Атрибут геоданных** выберите, какие географические сведения, соответствующие считанному IP-адресу, необходимо записать в событие. Доступные атрибуты геоданных: **Страна**, **Регион**, **Город**, **Долгота**, **Широта**.

   - В поле **Поле события для записи** выберите поле события, в которое необходимо записать выбранный атрибут геоданных.

   С помощью кнопки **Добавить атрибут геоданных** вы можете добавить пары полей **Атрибут геоданных** – **Поле события для записи**. Так вы можете настроить запись разных типов геоданных одного IP-адреса в разные поля события.

3. Для добавления каждого последующего сопоставления используйте кнопку **Добавить сопоставление** и повторяйте предыдущие два пункта инструкции.

   Вы можете записать одинаковые атрибуты геоданных в разные поля событий. Если вы настроите запись нескольких атрибутов геоданных в одно поле события, событие будет обогащено последним по очереди сопоставлением.

проверка DLL Hijacking

DLL Hijacking – это техника атаки, которая заключается в том, что на целевую систему доставляется уязвимое легитимное программное обеспечение вместе с вредоносной динамической библиотекой (DLL). Для обнаружения таких атак Kaspersky SIEM Cloud использует модуль AI. Модуль AI анализирует параметры запуска и исполнения программ и определяет подозрительные случаи запуска легитимного программного обеспечения с вредоносными библиотеками.

Для получения заключения Kaspersky SIEM Cloud отправляет запрос с информацией из полей события в <KSN>. В ответ на запрос KSN присылает результат анализа.

Вы можете настроить обнаружение атак DLL Hijacking в коллекторе или коррелляторе.

Для использования обогащения типа **Проверка DLL Hijacking** ваша лицензия должна включать в себя модуль AI. Главному администратору также требуется принять дополнительное Положение о KSN в блоке **Kaspersky Security Network** (**Параметры → KUMA → Открыть параметры KUMA → Интеграции → AI-сервисы → Обнаружение атак DLL Hijacking**).

Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "DLL Hijacking"

Параметр	Описание
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Укажите целое положительное число от 0 до 999. Если указано 0, то используется число логических ядер CPU.
Максимальный размер кеша	Максимальный размер кеша для ответов, получаемых из KSN, в мегабайтах. Значение по умолчанию: `128 МБ`. Каждый ответ из KSN имеет свое время жизни, в течение которого он хранится в кеше. Если Kaspersky SIEM Cloud отправляет повторный запрос по файлу DLL, для которого KSN уже выдал ответ, и время жизни этого ответа еще не истекло, то запрос не отправляется в KSN, а ответ берется из кеша.
Максимальное количество событий в очереди обогащения	При превышении указанного значения, новые события обрабатываться не будут. Значение по умолчанию: `1 000 000`. Значение `0` означает, что при возникновении очереди события перестают обогащаться.

Выполнять повторный запрос	В ответе KSN может выдать заключение **В обработке**. Этот заключение означает, что KSN принял запрос и в данный момент обрабатывает его, но заключения пока нет. Обработка может занять длительное время, поэтому требуется повторная отправка запроса.
	Если этот параметр включен, настройте дополнительные параметры:
	• **Создавать дубликаты событий** – если этот параметр включен, Kaspersky SIEM Cloud создает дубликат события и использует его для повторных запросов к KSN. Основное событие при этом отправляется дальше по потоку. Дубликат события будет записан в базу данных, когда выполнится одно из следующих условий:
	  • Из KSN получено заключение, отличное от **В обработке**.
	  • Переполнен дисковый буфер, размер которого указан в параметре **Размер буфера**.
	  • Превышено значение, указанное в параметре **Количество запросов**.
	  Если этот параметр выключен, Kaspersky SIEM Cloud продолжит отправлять запросы с использованием основного события. Событие будет записано в базу данных, когда выполнится одно из следующих условий:
	  • Из KSN получено заключение, отличное от **В обработке**.
	  • Переполнен дисковый буфер, размер которого указан в параметре **Размер буфера**.
	  • Превышено значение, указанное в параметре **Количество запросов**.
	• **Количество запросов** – максимальное количество запросов в KSN. Если за указанное количество запросов так и не будет получено заключение, отличное от **В обработке**, событие будет записано в базу данных с заключением **В обработке**. Значение по умолчанию: `10`.
	• **Интервал запросов** – интервал между запросами, в минутах. Значение по умолчанию: `1 минута`. Минимальное значение: `1 минута`.
	• **Размер буфера** – размер дискового буфера, который используется для хранения событий, ожидающих повторного запроса, в мегабайтах. Значение по умолчанию: `10240 МБ`. Минимальное значение: `10 МБ`.

Прокси-сервер	Параметры прокси-сервера, если он требуется для подключения к серверу KSN. Можно выбрать один из доступных или создать новый прокси-сервер. По умолчанию прокси-сервер не используется.
Сопоставление	Таблица параметров, которые нужно отправить в запросе в KSN для получения заключения, и соответствующих полей событий Kaspersky SIEM Cloud: • **Хеш файла DLL (md5)** – рекомендованное поле для сопоставления: `OldFileHash`. • **Путь до файла DLL** – полный путь, включающий имя файла. Рекомендованное поле для сопоставления: `OldFilePath`. Так как путь может содержать персональные данные, Kaspersky SIEM Cloud передает этот параметр в KSN в обезличенном виде. Например: Путь до обезличивания: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll` Тот же путь в обезличенном виде: `device\harddiskvolume1\users\username` • **Хеш процесса (md5)** – рекомендованное поле для сопоставления: `FileHash`. • **Путь до процесса** – полный путь, включающий имя файла. Так как путь может содержать персональные данные, Kaspersky SIEM Cloud передает этот параметр в KSN в обезличенном виде. Например: Путь до обезличивания: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll` Тот же путь в обезличенном виде: `device\harddiskvolume1\users\username` • **Имя файла DLL** – рекомендованное поле для сопоставления: `OldFileName`. • **Имя процесса** – рекомендованное поле для сопоставления: `FileName`. • **Подпись процесса** – поле, в котором указывается поле Kaspersky SIEM Cloud, которое передает `Organization` из `Subject` подписи. Если этих значений нет, подпись стоит оставить пустой. Чтобы добавить этот параметр, нажмите на кнопку **Добавить**, затем в столбце **Поле DLL Hijacking** в выпадающем списке выберите **подпись процесса**.необязательный параметр. Рекомендованное поле для сопоставления: FileID. • **Размер файла DLL** – необязательный параметр; рекомендованное поле для сопоставления: OldFileSize. Чтобы добавить этот параметр, нажмите на кнопку **Добавить**, затем в столбце **Поле DLL Hijacking** в выпадающем списке выберите **размер файла DLL**. Для каждого параметра укажите в таблице соответствующее ему поле события Kaspersky SIEM Cloud.

d. В раскрывающемся списке **Целевое поле** выберите поле события Kaspersky SIEM Cloud, в которое требуется поместить данные. Вы не можете выбрать значение, если в раскрывающемся списке **Исходный тип** вы выбрали **таблица**.

e. Если вы хотите включить детализацию в журнале нормализатора, включите переключатель **Отладка**. По умолчанию переключатель выключен.

6. Нажмите на кнопку **OK**.

Нормализатор будет создан и отобразится в виде темного кружка на вкладке мастера установки **Парсинг событий**. Вы можете нажать на темный кружок, чтобы просмотреть параметры нормализатора. Если вы хотите настроить параметры дополнительного парсинга наведите курсор на темный кружок и нажмите на отобразившийся значок плюса. Откроется окно **Дополнительный парсинг событий** с параметрами дополнительного парсинга. Подробнее о настройке параметров дополнительного парсинга событий см. ниже в разделе **Создание структуры правил нормализации событий**.

При отображении схемы нормализации структура вложенных нормализаторов не отображается. Чтобы ее просмотреть, нужно перейти в карточку нормализатора по ссылке с его названием. Если вы используете вложенный нормализатор с дополнительной нормализацией, нужно учитывать, что структура выходных данных может меняться. В этом случае важно понимать, какое поле будет передаваться другому дополнительному нормализатору.

4 Добавление фильтра (необязательный этап)

Вы можете создать фильтр, в параметрах которого будут определены условия отбора событий. В коллектор можно добавить несколько фильтров. Фильтры можно менять местами, перетягивая их мышью за значок ⣿, и удалять. Фильтры объединены оператором И.

Мы рекомендуем придерживаться выбранной схемы нормализации, когда вы указываете фильтры. Используйте в фильтрах только служебные поля Kaspersky SIEM Cloud и те поля, которые вы указали в нормализаторе в разделе **Сопоставление** и **Обогащение**. Например, если в нормализации не используется поле `DeviceAddress`, избегайте использования поля `DeviceAddress` в фильтре, поскольку такая фильтрация не сработает.

Чтобы создать фильтр:

1. В разделе **Фильтрация событий** нажмите на кнопку **Добавить фильтр** и в раскрывающемся меню **Фильтр** выберите пункт **Создать**.

2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого фильтра. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В блоке параметров **Условия** задайте условия, которым должны соответствовать отсеиваемые события:

   С помощью кнопки **Добавить условие** добавляются условия фильтра, можно выбрать два значения (левый и правый операнды) и назначить операцию, которую вы хотите выполнить с выбранными значениями. Результат операции – Истина (True) или Ложь (False).

   a. В раскрывающемся списке **оператор** необходимо выбрать функцию, которую должен выполнять фильтр.

      В этом же раскрывающемся списке можно установить флажок **без учета регистра**, если требуется, чтобы оператор игнорировал регистр значений. Флажок игнорируется, если выбраны операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

      Операторы фильтров

      - **=** – левый операнд равен правому операнду.
      - **<** – левый операнд меньше правого операнда.

- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

b. В раскрывающихся списках **Левый операнд** и **Правый операнд** необходимо выбрать, откуда поступят данные, с которыми произведет действие фильтр. В результате выбора появляются дополнительные параметры, с помощью которых необходимо точно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.

c. С помощью раскрывающегося списка **Если** можно выбрать, требуется ли создать отрицательное условие фильтра.

   Условие можно удалить с помощью кнопки ×.

d. С помощью кнопки **Добавить группу** добавляются группы условий. Оператор **И** можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

   Группу условий можно удалить с помощью кнопки ×.

e. С помощью кнопки **Добавить фильтр** в условия добавляются существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**. В параметры вложенного фильтра можно перейти с помощью кнопки ↗.

Фильтр добавлен. Его можно удалить с помощью кнопки ×.

5 Добавление правила агрегации (необязательный этап)

1. В разделе **Агрегация событий** нажмите на кнопку **Добавить правило агрегации**.

2. В раскрывающемся меню **Правило агрегации** выберите нужное правило или создайте новое, нажав **Создать**.

3. В поле **Название** введите название для создаваемого правила агрегации. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В поле **Предел событий** укажите количество событий, которое должно быть получено, чтобы сработало правило агрегации и события были объединены. Значение по умолчанию: `100`.

5. В поле **Время ожидания событий** укажите количество секунд, в течение которых коллектор получает события для объединения. По истечении этого срока правило агрегации срабатывает и создается новое агрегационное событие. Значение по умолчанию: `60`.

6. В поле **Группирующие поля** с помощью кнопки **Добавить поле** выберите поля, по которым будут определяться однотипные события. Вы можете выбрать следующие служебные поля: SourceAssetID, DestinationAssetID, DeviceAssetID, SourceAccountID, DestinationAccountID. Идентификаторы активов добавляются после нормализации события, поэтому по ним можно будет агрегировать события. Остальные служебные поля не используются в агрегации. Выбранные события можно удалять с помощью кнопок со значком крестика.

7. В поле **Уникальные поля** с помощью кнопки **Добавить поле** можно выбрать поля, при наличии которых коллектор исключит событие из процесса агрегации даже при наличии полей, указанных в разделе **Группирующие поля**. Выбранные события можно удалять с помощью кнопок со значком крестика.

8. В поле **Поля суммы** с помощью кнопки **Добавить поле** можно выбрать поля, значения которых будут просуммированы в процессе агрегации. Выбранные события можно удалять с помощью кнопок со значком крестика.

9. В блоке параметров **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр.

   Создание фильтра в ресурсах

   Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

   Чтобы создать фильтр:

   1. В раскрывающемся списке **Фильтр** выберите **Создать**.

   2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят.

   3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.

   4. Выберите режим создания фильтра: **Конструктор** или **Код**.

      При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра.

   5. Если вы выбрали вариант **Конструктор**, выполните следующие действия:

      a. В раскрывающемся списке выберите логический оператор:

         - **И** – отбирает события, которые соответствуют всем указанным условиям.
         - **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий.
         - **НЕ** – отбирает события, которые не соответствуют всем указанным условиям.

      b. Нажмите на кнопку **Добавить условие**.

      c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

      d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра.

Операнды фильтров

- **Поля событий** – поле события, которое требуется использовать как операнд фильтра.
- **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**.

  Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра.
- **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры:
  - **словарь** (обязательно) – словарь, который требуется использовать.
  - **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.
- **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события.
  - **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать.
  - **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы.
  - **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда.
  - **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда.
- **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
  - **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**.
  - **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.
- **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
  - **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
  - **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
  - **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.

- **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
  - **значение** (обязательно) – константа, которую требуется присвоить операнду.
- **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
  - **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.

Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в коррелляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.

Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.

e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.

Вы можете добавить несколько групп условий.

6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.

В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕.

8. Нажмите **Сохранить**.

Правило агрегации будет добавлено. Его можно удалить с помощью кнопки ✕.

6 Обогащение событий (необязательный этап)

Вы можете указать, какими данными и из каких источников следует дополнить обрабатываемые коллектором события. События можно обогащать данными, полученными с помощью правил обогащения или с помощью LDAP.

Поступающие события сначала обогащаются данными из источников, которые вы выбираете на этом шаге мастера, а затем выполняется автоматическое обогащение данными об активах. Например, если у вас настроено dns-обогащение и в результате IP-адрес, указанный в событии, обогатился соответствующим DNS-именем актива, то произойдет обогащение события этим активом.

Коллектор получает сведения об активах от Ядра Kaspersky SIEM Cloud и обогащает ими события следующим образом:

- Если в поле события с именем (например, `SourceHostName`) содержится FQDN, совпадающий с FQDN актива, коллектор добавляет поле `SourceAssetID` с идентификатором этого актива. Значение поля `SourceAddress` при этом не учитывается.

- Если в поле события с IP-адресом (например, `DestinationAddress`) указан IP-адрес актива, а поле с именем пустое, коллектор добавляет поле `DestinationAssetID` с идентификатором актива, IP-адрес которого совпадает.

- Если в поле события с именем есть значение, которое не совпадает ни с одним FQDN из базы активов, коллектор не проверяет поле с IP-адресом и не добавляет идентификатор актива. Это относится как к случаям, когда в поле `HostName` указан FQDN, который не соответствует ни одному активу, так и к ситуациям, когда в поле `HostName` указано неполное имя (например, только имя хоста без домена).

Правил обогащения может быть несколько. Их можно добавить с помощью кнопки **Добавить обогащение** или удалить с помощью кнопки ✕. Можно использовать существующие правила обогащения или же создать новые правила.

Чтобы создать правило обогащения:

1. Откройте раздел **Обогащение событий**.

2. В зависимости от того, с помощью чего вы хотите обогащать события, выполните следующие действия:

   - Если вы хотите обогащать события данными, полученными с помощью правил обогащения, выполните следующие действия:

     a. Нажмите **Добавить обогащение**.

     Откроется блок параметров правил обогащения.

     b. В поле **Название** введите уникальное имя правила. Название должно содержать от 1 до 128 символов в кодировке Unicode.

     c. В раскрывающемся списке **Правило обогащения** выберите **Создать**.

     d. В раскрывающемся списке **Тип источника данных** выберите, откуда будут поступать данные для обогащения, и заполните относящиеся к нему параметры:

     шаблон

     Этот тип обогащения используется, если в поле события нужно записать значение, полученное при обработке шаблонов Go. Мы рекомендуем сопоставлять значение и размер поля. Параметры этого типа обогащения описаны в таблице ниже.

     Параметры типа обогащения "шаблон"

Параметр	Описание
Шаблон	Шаблон Go. Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт, например `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.
Целевое поле	Поле события, в которое требуется поместить данные.

Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **шаблон**, целевым полем является поле с типом `Строка`, а исходным полем является поле расширенной схемы событий, содержащее массив строк, то в шаблоне может быть использован один из следующих примеров:

- `{{.SA.StringArrayOne}}`
- ```
  {{- range $index, $element := . SA.StringArrayOne -}}
  {{- if $index}}, {{end}}"{{$element}}"{{- end -}}
  ```

Для преобразования в шаблоне данных поля массива в формат TSV требуется использовать функцию `toString`, например:

```
template {{toString .SA.StringArray}}
```

таблица

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "таблица"

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.
Сопоставление	Поля событий для передачи данных: • **Поле словаря** – поля словаря, из которых будут передаваться данные. Доступные поля зависят от выбранного ресурса словаря. • **Поле KUMA** – поля событий, в которые будут передаваться данные. Для выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** вы можете задать название для помещаемых данных.

Первое поле в таблице (**Поле словаря**) считается ключом, с которым будут сопоставляться поля, выбранные из события в качестве ключевых (**Поле KUMA**). В качестве ключа в **Поле словаря** вам нужно выбрать индикатор компрометации, по которому будет осуществляться обогащение, например IP-адрес, URL-адрес или хеш. В правиле необходимо выбрать поле события, соответствующее выбранному индикатору в поле словаря.

Если вы хотите выбрать несколько ключевых полей, вы можете указать их через разделитель `|` (при указании через веб-интерфейс или импорте через CSV-файл), например `<IP-адрес>|<имя пользователя>`.

Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить**. Для удаления строки таблицы нажмите на крестик ✕.

обогащение активами

Этот тип обогащения используется, когда необходимо добавить обогащение событий активами на определенных коллекторах.

Для обогащения событий активами в блоке **Сопоставление** требуется заполнить таблицу сопоставления полей события Kaspersky SIEM Cloud и полей для записи значениий из хеш-таблицы.
```

Чтобы заполнить таблицу сопоставления полей:

1. В блоке **Сопоставление** нажмите на кнопку **Добавить**.

2. В раскрывающемся списке **Поле KUMA** выберите одно или несколько полей события, значение которого будет сопоставляться со значением из хеш-таблицы и записываться в соответствующее поле в таблице данных актива.

3. В раскрывающемся списке **Поле для записи данных** выберите поле, в которое при соответствии поля события (**Поле KUMA**) и значения из хеш-таблицы будет записано значение идентификатора актива.

   Возможные значения параметров в таблице сопоставления полей

Поле KUMA	Поле для записи данных

`DestinationAddress`
`DestinationHostName`
`DeviceAddress`
`DeviceHostName`
`SourceAddress`
`SourceHostName`
`DestinationMacAddress`
`DeviceMacAddress`
`SourceMacAddress`
`DeviceCustomString1`
`DeviceCustomString2`
`DeviceCustomString3`
`DeviceCustomString4`
`DeviceCustomString5`
`DeviceCustomString6`
	`SourceAssetID`
	`DeviceAssetID`
	`DestinationAssetID`

   Если вы указываете несколько полей, к значениям полей применяется условие **И**. Если вы добавляете несколько строк в столбце **Поле KUMA**, к значениям полей применяется условие **ИЛИ**. Проверка начинается с первого поля в списке. Если значение поля совпадает со значением атрибута, проверка прекращается.

   Например, в событие поступают следующие данные:

   `SourceAddress=192.168.x.xx`
   `SourceHostName=kuma.example.com`

   В Kaspersky SIEM Cloud есть два актива: `company.example.com` (IP-адрес: `192.168.x.xx`; FQDN: `company.example.com`) и `kuma.example.com` (IP-адрес: `192.168.y.yyy`; FQDN: `kuma.example.com`). Сопоставление для них осуществляется следующим образом:

   - Если вы указали отдельно `sourceAddress` → `sourceAssetID`, а затем `sourceHostname` → `sourceAssetID`, то актив будет соответствовать первому условию (`company.example.com`).
   - Если вам важнее получить значение параметра `sourceHostname` (`kuma.example.com`), то первым указывается `sourceHostname` → `sourceAssetID`, а затем `sourceAddress` → `sourceAssetID`.
   - Если вы указали `sourceAddress` + `sourceHostname` → `sourceAssetID`, обогащение не произойдет.

   В таблице сопоставления полей требуется указать хотя бы одно условие сопоставления.

4. Если вы хотите применить для параметров **Поле KUMA** и **Поле для записи данных** значения по умолчанию, нажмите на кнопку. **Применить сопоставление по умолчанию**, расположенную над таблицей.

   Значения параметров по умолчанию

Поле KUMA	Поле для записи данных
DestinationAddress	DestinationAssetID
DestinationHostName	DestinationAssetID
DeviceAddress	DeviceAssetID
DeviceHostName	DeviceAssetID
SourceAddress	SourceAssetID
SourceHostName	SourceAssetID

константа

Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "константа"

Параметр	Описание
Константа	Значение, которое требуется добавить в поле события. Максимальная длина значения – до 255 символов в кодировке Unicode. Если оставить поле пустым, существующее значение поля события будет удалено.
Целевое поле	Поле события, в которое требуется поместить данные.

Если вы используете функции обогащения событий для полей расширенной схемы с типом `Строка`, `Число` или `Число с плавающей точкой` с помощью константы, в поле будет добавлена константа.

Если вы используете функции обогащения событий для полей расширенной схемы с типом `Массив строк`, `Массив чисел` или `Массив чисел с плавающей точкой` с помощью константы, константа будет добавлена к элементам массива.

словарь

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "словарь"

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.

Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **словарь**, а в параметре **Ключевые поля обогащения** указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку в соответствии с правилами сериализации одного значения в формате TSV.

Пример. В параметре **Ключевые поля обогащения** используется поле расширенной схемы `SA.StringArrayOne`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`. В качестве ключа в словарь будут переданы значения `['a','b','c']`.

Если в параметре **Ключевые поля обогащения** используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом `|`.

Пример. В параметре **Ключевые поля обогащения** используется поле расширенной схемы `SA.StringArrayOne` и строковое поле `Code`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`, а строковое поле `Code` содержит последовательность символов `myCode`. В качестве ключа в словарь будут переданы значения `['a','b','c']|myCode`.

событие

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры типа обогащения описаны в таблице ниже.

Параметры типа обогащения "событие"

Параметр	Описание
Целевое поле	Поле события, в которое следует поместить данные.
Исходное поле	Поле события, значение которого будет записано в целевое поле.
Преобразование	Блок параметров, в котором можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий. Тип преобразования можно выбрать в раскрывающемся списке. С помощью кнопок **Добавить преобразование** и **Удалить** можно добавить или удалить преобразование. Порядок преобразований имеет значение.

Возможность использовать преобразования зависит от типа используемого поля расширенной схемы событий:

- Для дополнительного поля с типом `Строка` доступны все типы преобразования.
- Для полей с типами `Число` и `Число с плавающей точкой` доступны типы преобразования **regexp**, **substring**, **replace**, **trim**, **append**, **prepend**, **replaceWithRegexp**, **decodeHexString**, **decodeBase64String** и **decodeBase64URLString**.
- Для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны типы преобразования **append** и **prepend**.

Посмотреть доступные преобразования

Преобразования – это изменения, которые применяются к значению перед записью в поле события.

Вы можете выбрать в раскрывающемся списке один из следующих типов преобразования:

- **entropy** – используется для преобразования значения исходного поля с помощью функции вычисления информационной энтропии и помещения результата преобразования в целевое поле типа `float`. Результатом преобразования будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например, когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.
- **lower** – используется для перевода всех символов значения в нижний регистр.
- **upper** – используется для перевода всех символов значения в верхний регистр.
- **regexp** – используется для преобразования значения с помощью указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.
- **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Символы на замену** – последовательность символов, которую требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

- **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` требуется выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.

- **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

- Конвертация закодированных строк в текст:

  - **decodeHexString** – используется для конвертации HEX-строки в текст.

  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  - **unicodeUnescape** – используется для конвертации Unicode-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.

  Мы не рекомендуем использовать несколько дополнительных нормализаторов для последовательного преобразования одного и того же поля. Результат одного преобразования, выполненного дополнительным нормализатором, не используется как входные данные для следующего. В итоговое событие записывается значение, полученное в дополнительном нормализаторе, который первым выполнил обогащение этого поля.

- Преобразование формата IP-адреса в IPv4:
  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
- **hexToDecimal** – используется для преобразования числового значения, представленного в шестнадцатеричной системе счисления, в десятичный формат. Преобразование применяется к строковым или числовым полям, содержащим HEX-значения (включая префикс 0x, если он присутствует), и результат записывается в целевое поле события Kaspersky SIEM Cloud в виде целого числа.

  Результатом преобразования является число в десятичной системе, например исходное значение – 0x00FF, после преобразования – 255.

dns

Этот тип обогащения используется для отправки запросов на DNS-сервер частной сети для преобразования IP-адресов в доменные имена или наоборот. Преобразование IP-адресов в DNS-имена происходит только для частных адресов: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10, fd00::/8.

Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "dns"

Параметр	Описание
URL	URL DNS-сервера, которому вы хотите отправлять запросы. С помощью кнопки **Добавить URL** можно указать несколько URL. Если параметр **URL** не указан, то Kaspersky SIEM Cloud возьмет список DNS-серверов из файла `/etc/resolv.conf`, расположенного на локальном хосте. В этом случае вам нужно включить параметр **Требуется рекурсия**. В противном случае обогащение происходить не будет.
Запросов в секунду	Максимальное количество запросов к DNS-серверу в секунду. Значение по умолчанию: количество vCPU сервера, на котором установлено Ядро Kaspersky SIEM Cloud.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Укажите целое положительное число от 0 до 999. Если указано 0, то используется число логических ядер CPU. Значение по умолчанию: `1`.
Максимальное число событий в очереди обогащения	Максимальное число событий, сохраняемое в очереди для повторной отправки. Значение по умолчанию: `1 000 000`.
Время ожидания	Время ожидания ответа от DNS-сервера (в секундах). Значение по умолчанию: `5`.
Переопределение режима DNS	Используемый метод преобразования: - **Только прямое разрешение DNS** – доменное имя преобразуется в IP-адрес. - **Только обратное разрешение DNS** – IP-адрес преобразуется в доменное имя. - **Прямое и обратное DNS-разрешение** – доменное имя может преобразовываться в IP-адрес и наоборот.
Срок жизни кеша	Время жизни значений (в секундах), хранящихся в кеше. Значение по умолчанию: `60` (сек).
Кеш отключен	Параметр, позволяющий включить или выключить кеширование. По умолчанию кеширование включено.
Обновление кэша отключено	Если обновление кеша включено, то по истечении срока жизни кеша коллектор отправляет повторные запросы на DNS-сервер для обновления хранящихся в кеше данных. Этот параметр доступен только при включенном кеше. По умолчанию обновление кеша включено.
Требуется рекурсия	Параметр позволяет включить отправку коллектором рекурсивных запросов к авторитативным DNS-серверам для выполнения обогащения. Значение по умолчанию: **Выключено**.

cybertrace

Для систем с большой нагрузкой на коллектор или коррелятор рекомендуется использовать тип обогащения **cybertrace-http**. Этот тип обогащения возвращает структурированный ответ в формате JSON и корректно различает строки и массивы пользовательских атрибутов, исключая ошибки парсинга.
При обогащении с помощью типа **cybertrace** коллектор получает неструктурированный ответ. Если значение пользовательского атрибута в Kaspersky CyberTrace содержит квадратные скобки, например **[str1**, **str2]**, Kaspersky SIEM Cloud обрабатывает его как массив, а не как строку.

Этот тип обогащения используется для добавления в поля события сведений из потоков данных Kaspersky CyberTrace. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "cybertrace"

Параметр	Описание
URL	URL сервера Kaspersky CyberTrace, которому вы хотите отправлять запросы. Порт Kaspersky CyberTrace по умолчанию: 9999. Обязательный параметр.
Количество подключений	Максимальное количество подключений к серверу Kaspersky CyberTrace, которые может одновременно установить Kaspersky SIEM Cloud. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро Kaspersky SIEM Cloud.
Запросов в секунду	Максимальное количество запросов к серверу в секунду. Значение по умолчанию: `1000`.
Время ожидания	Время ожидания отклика от сервера Kaspersky CyberTrace в секундах. Значение по умолчанию: `30`.
Максимальное кол-во событий в очереди обогащения	Максимальное количество событий, сохраняемое в очереди для переотправки. Значение по умолчанию: `1 000 000`.
Сопоставление	Таблица сопоставления полей событий с типами индикаторов Kaspersky CyberTrace. В столбце **Поле KUMA** указаны названия полей событий, а в столбце **Индикатор CyberTrace** указаны типы индикаторов Kaspersky CyberTrace. Доступные типы индикаторов Kaspersky CyberTrace: • **ip** • **url** • **hash**

В таблице сопоставления требуется указать как минимум одну строку. Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить строку**. Для удаления строки таблицы нажмите на крестик ×.

cybertrace-http

Этот тип потокового обогащения событий в Kaspersky CyberTrace, который позволяет отправлять большое количество событий одним запросом на API-интерфейс CyberTrace. Мы рекомендуем применять тип обогащения **cybertrace-http** в системах с большим потоком событий. Производительность **cybertrace-http** превосходит показатели типа обогащения **cybertrace**.

Ограничения:

- Тип обогащения **cybertrace-http** невозможно использовать для ретроспективного сканирования в KUMA.

- В случае использования типа обогащения **cybertrace-http** обнаружения киберугроз не сохраняются в истории Kaspersky CyberTrace в окне **Обнаружения**.

Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "cybertrace-http"

Параметр	Описание
Тенант	Тенант, в рамках которого вы планируете работать с Kaspersky CyberTrace. Обязательный параметр.
URL	URL сервера Kaspersky CyberTrace, которому вы хотите отправлять запросы и порт, который использует API CyberTrace. Порт по умолчанию 443. Обязательный параметр.
Секрет	Раскрывающийся список для выбора секрета, в котором хранятся учетные данные для подключения. Обязательный параметр.
Время ожидания	Время ожидания отклика от сервера Kaspersky CyberTrace в секундах. Значение по умолчанию: `30`.
Ключевые поля	Список полей событий, используемых для обогащения событий данными из Kaspersky CyberTrace. Обязательный параметр.
Максимальное кол-во событий в очереди обогащения	Максимальное количество событий, сохраняемое в очереди для переотправки. Значение по умолчанию: `1 000 000`. По достижении 1 млн получаемых событий от сервера Kaspersky CyberTrace события перестают обогащаться, пока число получаемых событий не станет меньше 500 тыс.
Основная версия CyberTrace	Версия Kaspersky CyberTrace. Доступные значения: • **<5** – запросы будут выполняться в тенанте General в Kaspersky CyberTrace и будут использовать новую версию API, соответствующую Kaspersky CyberTrace 5.0 и выше. • **≥ 5.0** – запросы будут использовать версию API, соответствующую Kaspersky CyberTrace 4.x. Значение по умолчанию: **<5**.
Отладка	Параметр, включающий логирование ресурса. По умолчанию переключатель выключен.
Теги	Теги для поиска ресурса.

часовой пояс

Этот тип обогащения используется в коллекторах и коррелляторах, чтобы присвоить событию определенный часовой пояс. Сведения о часовом поясе могут понадобиться при поиске событий, случившихся в нетипичное время, например ночью.

При выборе этого типа обогащения в раскрывающемся списке **Часовой пояс** нужно указать временную зону.

> Убедитесь, что выбираемый часовой пояс установлен на сервере сервиса, использующего обогащение. Например, это можно сделать с помощью команды `timedatectl list-timezones`, которая показывает все установленные на сервере часовые пояса. Подробнее об установке часовых поясов смотрите в документации используемой вами операционной системы.

При обогащении события в поле события DeviceTimeZone записывается смещение времени выбранного часового пояса относительно всемирного координированного времени (UTC) в формате `+-чч:мм`. Например, если выбрать временную зону **Asia/Yekaterinburg** в поле `DeviceTimeZone` будет записано значение `+05:00`. Если в обогащаемом событии есть значение поля `DeviceTimeZone`, оно будет перезаписано.

По умолчанию, если в обрабатываемом событии не указан часовой пояс и не настроены правила обогащения по часовому поясу, событию присваивается часовой пояс сервера, на котором установлен сервис (коллектор или коррелятор), обрабатывающий событие. При изменении времени сервера сервис требуется перезапустить.

Допустимые форматы времени при обогащении поля DeviceTimeZone

При обработке в коллекторе поступающих сырых событий следующие форматы времени могут быть автоматически приведены к формату `+-чч:мм` (см. таблицу ниже):

Формат времени в обрабатываемом событии	Пример
+-чч:мм	-07:00
+-ччмм	-0700
+-чч	-07

Если формат даты в поле `DeviceTimeZone` отличается от указанных в таблице, при обогащении события сведениями о часовом поясе в поле записывается часовой пояс серверного времени коллектора. Вы можете создать правила нормализации для нестандартных форматов времени.

геоданные

Этот тип обогащения используется для добавления в поля событий сведений о географическом расположении IP-адресов.

При выборе этого типа в блоке параметров **Сопоставление геоданных с полями события** укажите, из какого поля события будет считан IP-адрес, а также выберите атрибуты геоданных и определите поля событий, в которые геоданные будут записаны:

1. В раскрывающемся списке **Поле события с IP-адресом** выберите поле события, из которого считывается IP-адрес. По этому IP-адресу будет произведен поиск соответствий по загруженным в Kaspersky SIEM Cloud геоданным.

   При выборе полей события `SourceAddress`, `DestinationAddress` и `DeviceAddress` становится доступна кнопка **Применить сопоставление по умолчанию**. С ее помощью можно добавить преднастроенные пары соответствий атрибутов геоданных и полей события.

2. Для каждого поля события, откуда требуется считать IP-адрес, выберите тип геоданных и поле события, в которое следует записать геоданные.

   - В поле **Атрибут геоданных** выберите, какие географические сведения, соответствующие считанному IP-адресу, необходимо записать в событие. Доступные атрибуты геоданных: **Страна**, **Регион**, **Город**, **Долгота**, **Широта**.
   - В поле **Поле события для записи** выберите поле события, в которое необходимо записать выбранный атрибут геоданных.

   С помощью кнопки **Добавить атрибут геоданных** вы можете добавить пары полей **Атрибут геоданных** – **Поле события для записи**. Так вы можете настроить запись разных типов геоданных одного IP-адреса в разные поля события.

3. Для добавления каждого последующего сопоставления используйте кнопку **Добавить сопоставление** и повторяйте предыдущие два пункта инструкции.

   Вы можете записать одинаковые атрибуты геоданных в разные поля событий. Если вы настроите запись нескольких атрибутов геоданных в одно поле события, событие будет обогащено последним по очереди сопоставлением.

проверка DLL Hijacking

DLL Hijacking – это техника атаки, которая заключается в том, что на целевую систему доставляется уязвимое легитимное программное обеспечение вместе с вредоносной динамической библиотекой (DLL). Для обнаружения таких атак Kaspersky SIEM Cloud использует модуль AI. Модуль AI анализирует параметры запуска и исполнения программ и определяет подозрительные случаи запуска легитимного программного обеспечения с вредоносными библиотеками.

Для получения заключения Kaspersky SIEM Cloud отправляет запрос с информацией из полей события в <KSN>. В ответ на запрос KSN присылает результат анализа.

Вы можете настроить обнаружение атак DLL Hijacking в коллекторе или коррелляторе.

Для использования обогащения типа **Проверка DLL Hijacking** ваша лицензия должна включать в себя модуль AI. Главному администратору также требуется принять дополнительное Положение о KSN в блоке **Kaspersky Security Network** (**Параметры** → **KUMA** → **Открыть параметры KUMA** → **Интеграции** → **AI-сервисы** → **Обнаружение атак DLL Hijacking**).

Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "DLL Hijacking"

Параметр	Описание
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Укажите целое положительное число от 0 до 999. Если указано 0, то используется число логических ядер CPU.
Максимальный размер кеша	Максимальный размер кеша для ответов, получаемых из KSN, в мегабайтах. Значение по умолчанию: `128 МБ`. Каждый ответ из KSN имеет свое время жизни, в течение которого он хранится в кеше. Если Kaspersky SIEM Cloud отправляет повторный запрос по файлу DLL, для которого KSN уже выдал ответ, и время жизни этого ответа еще не истекло, то запрос не отправляется в KSN, а ответ берется из кеша.
Максимальное количество событий в очереди обогащения	При превышении указанного значения, новые события обрабатываться не будут. Значение по умолчанию: `1 000 000`. Значение `0` означает, что при возникновении очереди события перестают обогащаться.

Выполнять повторный запрос	В ответе KSN может выдать заключение **В обработке**. Этот заключение означает, что KSN принял запрос и в данный момент обрабатывает его, но заключения пока нет. Обработка может занять длительное время, поэтому требуется повторная отправка запроса.
	Если этот параметр включен, настройте дополнительные параметры:
	• **Создавать дубликаты событий** – если этот параметр включен, Kaspersky SIEM Cloud создает дубликат события и использует его для повторных запросов к KSN. Основное событие при этом отправляется дальше по потоку. Дубликат события будет записан в базу данных, когда выполнится одно из следующих условий:
	  • Из KSN получено заключение, отличное от **В обработке**.
	  • Переполнен дисковый буфер, размер которого указан в параметре **Размер буфера**.
	  • Превышено значение, указанное в параметре **Количество запросов**.
	  Если этот параметр выключен, Kaspersky SIEM Cloud продолжит отправлять запросы с использованием основного события. Событие будет записано в базу данных, когда выполнится одно из следующих условий:
	  • Из KSN получено заключение, отличное от **В обработке**.
	  • Переполнен дисковый буфер, размер которого указан в параметре **Размер буфера**.
	  • Превышено значение, указанное в параметре **Количество запросов**.
	• **Количество запросов** – максимальное количество запросов в KSN. Если за указанное количество запросов так и не будет получено заключение, отличное от **В обработке**, событие будет записано в базу данных с заключением **В обработке**. Значение по умолчанию: `10`.
	• **Интервал запросов** – интервал между запросами, в минутах. Значение по умолчанию: `1 минута`. Минимальное значение: `1 минута`.
	• **Размер буфера** – размер дискового буфера, который используется для хранения событий, ожидающих повторного запроса, в мегабайтах. Значение по умолчанию: `10240 МБ`. Минимальное значение: `10 МБ`.

Прокси-сервер	Параметры прокси-сервера, если он требуется для подключения к серверу KSN. Можно выбрать один из доступных или создать новый прокси-сервер. По умолчанию прокси-сервер не используется.
Сопоставление	Таблица параметров, которые нужно отправить в запросе в KSN для получения заключения, и соответствующих полей событий Kaspersky SIEM Cloud: • **Хеш файла DLL (md5)** – рекомендованное поле для сопоставления: `OldFileHash`. • **Путь до файла DLL** – полный путь, включающий имя файла. Рекомендованное поле для сопоставления: `OldFilePath`. Так как путь может содержать персональные данные, Kaspersky SIEM Cloud передает этот параметр в KSN в обезличенном виде. Например: Путь до обезличивания: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll` Тот же путь в обезличенном виде: `device\harddiskvolume1\users\username` • **Хеш процесса (md5)** – рекомендованное поле для сопоставления: `FileHash`. • **Путь до процесса** – полный путь, включающий имя файла. Так как путь может содержать персональные данные, Kaspersky SIEM Cloud передает этот параметр в KSN в обезличенном виде. Например: Путь до обезличивания: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll` Тот же путь в обезличенном виде: `device\harddiskvolume1\users\username` • **Имя файла DLL** – рекомендованное поле для сопоставления: `OldFileName`. • **Имя процесса** – рекомендованное поле для сопоставления: `FileName`. • **Подпись процесса** – поле, в котором указывается поле Kaspersky SIEM Cloud, которое передает `Organization` из `Subject` подписи. Если этих значений нет, подпись стоит оставить пустой. Чтобы добавить этот параметр, нажмите на кнопку **Добавить**, затем в столбце **Поле DLL Hijacking** в выпадающем списке выберите **подпись процесса**.необязательный параметр. Рекомендованное поле для сопоставления: FileID. • **Размер файла DLL** – необязательный параметр; рекомендованное поле для сопоставления: OldFileSize. Чтобы добавить этот параметр, нажмите на кнопку **Добавить**, затем в столбце **Поле DLL Hijacking** в выпадающем списке выберите **размер файла DLL**. Для каждого параметра укажите в таблице соответствующее ему поле события Kaspersky SIEM Cloud.

e. Если требуется включить логирование операций сервиса, включите переключатель **Отладка**.

f. При необходимости в раскрывающемся списке **Теги** выберите теги для правила обогащения.

g. При необходимости в поле **Описание** добавьте описание правила обогащения. Описание правила может содержать до 4000 символов в кодировке Unicode.

h. Если вы хотите задать условия определения событий, которые будут обрабатываться с применением правила обогащения, в блоке **Параметры фильтра** в раскрывающемся списке **Фильтр** выберите или создайте фильтр.

Как создать фильтр

Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

Чтобы создать фильтр:

1. В раскрывающемся списке **Фильтр** выберите **Создать**.

2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят.

3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.

4. Выберите режим создания фильтра: **Конструктор** или **Код**.

   При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра.

5. Если вы выбрали вариант **Конструктор**, выполните следующие действия:

   a. В раскрывающемся списке выберите логический оператор:

      - **И** – отбирает события, которые соответствуют всем указанным условиям.
      - **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий.
      - **НЕ** – отбирает события, которые не соответствуют всем указанным условиям.

   b. Нажмите на кнопку **Добавить условие**.

   c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

   d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра.

Операнды фильтров

- **Поля событий** – поле события, которое требуется использовать как операнд фильтра.
- **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**.

  Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра.
- **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры:
  - **словарь** (обязательно) – словарь, который требуется использовать.
  - **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.
- **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события.
  - **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать.
  - **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы.
  - **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда.
  - **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда.
- **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
  - **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**.
  - **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.
- **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
  - **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
  - **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
  - **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.

- **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
  - **значение** (обязательно) – константа, которую требуется присвоить операнду.
- **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
  - **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.

Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в коррелляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.

Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.

e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.

Вы можете добавить несколько групп условий.

6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.

В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕.

8. Нажмите **Сохранить**.

- Если вы хотите обогащать события данными, полученными с помощью LDAP, выполните следующие действия:

a. Нажмите **Добавить сопоставление с учетными записями LDAP**.

Откроется блок параметров обогащения с помощью LDAP.

b. В поле **Сопоставление с учетными записями LDAP** добавьте одно или несколько названий подключений к LDAP-серверу, которые вы создавали в настройках интеграции с LDAP-сервером.

c. В таблице **Обогащение полей KUMA** задайте правила сопоставления полей Kaspersky SIEM Cloud с атрибутами LDAP:

- В столбце **Поле KUMA** укажите поле события Kaspersky SIEM Cloud, данные из которого следует сравнивать с атрибутом LDAP.
- В столбце **LDAP-атрибут**, укажите атрибут, с которым необходимо сравнивать поле события Kaspersky SIEM Cloud. Раскрывающийся список содержит часть стандартных атрибутов, по которым может быть выполнено обогащение. Список может быть дополнен пользовательскими атрибутами.

Настройка обогащения с помощью пользовательских атрибутов

Перед настройкой обогащения событий с помощью пользовательских атрибутов убедитесь, что пользовательские атрибуты настроены в AD.

Чтобы обогащать события учетными записями с помощью пользовательских атрибутов:

1. Добавьте **Пользовательские атрибуты учетных записей AD** в параметрах подключения к LDAP.

   Невозможно добавить стандартные импортируемые атрибуты из AD в качестве пользовательских. Например, если вы захотите добавить стандартный атрибут `accountExpires` в качестве пользовательского атрибута, при сохранении параметров подключения Kaspersky SIEM Cloud вернет ошибку.

   Список импортируемых атрибутов из AD

   Из Active Directory можно запросить следующие атрибуты учетных записей:

   - `accountExpires`
   - `badPasswordTime`
   - `cn`
   - `company`
   - `department`
   - `displayName`
   - `distinguishedName`
   - `division`
   - `employeeID`
   - `ipaUniqueID`
   - `l`
   - `mail`
   - `mailNickname`
   - `managedObjects`
   - `manager`
   - `memberOf` (по этому атрибуту события можно искать при корреляции)
   - `mobile`
   - `objectGUID` (этот атрибут запрашивается из Active Directory всегда)
   - `objectSid`
   - `physicalDeliveryOfficeName`

- `sAMAccountName`
- `sAMAccountType`
- `sn`
- `streetAddress`
- `telephoneNumber`
- `title`
- `userAccountControl`
- `userPrincipalName`
- `whenChanged`
- `whenCreated`

После того, как вы добавите пользовательские атрибуты в параметрах подключения к LDAP, раскрывающийся список **LDAP-атрибуты** в коллекторе будет автоматически дополнен. Пользовательские атрибуты можно отличить по знаку вопроса рядом с именем атрибута. Если для нескольких доменов вы добавили один и тот же атрибут, в раскрывающемся списке атрибут будет указан один раз, а домены можно просмотреть, если навести курсор на знак вопроса. Названия доменов отображаются в виде ссылок: если вы нажмете на ссылку, домен автоматически добавится в **Сопоставление с учетными записями LDAP**, если прежде он не был добавлен.

Если вы удалили пользовательский атрибут в параметрах подключения к LDAP, удалите вручную строку с атрибутом из таблицы сопоставления в коллекторе. Информация об атрибутах учетных записей в KUMA обновляется каждый раз после того, как вы выполните импорт учетных записей.

2. Импортируйте учетные записи.
3. В коллекторе в таблице **Обогащение полей KUMA** задайте правила сопоставления полей KUMA с атрибутами LDAP.
4. Перезапустите коллектор.

   После перезапуска коллектора Kaspersky SIEM Cloud начнет обогащать события учетными записями.

- В столбце **Поле для записи данных** укажите, в какое поле события Kaspersky SIEM Cloud следует помещать идентификатор пользовательской учетной записи, импортированной из LDAP, если сопоставление успешно.

С помощью кнопки **Добавить** в таблицу можно добавить строку, а с помощью кнопки **Удалить** – удалить. С помощью кнопки **Применить сопоставление по умолчанию** можно заполнить таблицу сопоставления стандартными значениями.

При добавлении в существующий коллектор обогащения с помощью LDAP или изменении параметров обогащения требуется остановить и запустить сервис снова.

❼ Добавление точки назначения (необязательный этап)

Вы можете выбрать или создать точки назначения, в параметрах которых будут определено, куда следует перенаправлять обработанные коллектором события. Обычно события от коллектора перенаправляются в коррелятор для анализа и поиска угроз и в хранилище для хранения, а также чтобы обработанные события можно было просматривать позднее. При необходимости события можно отправлять, например, в маршрутизатор событий. В этом случае следует выбрать коннектор `internal` на шаге **Транспорт**. Точек назначения может быть несколько.

Чтобы добавить точку назначения:

1. В разделе **Маршрутизация** нажмите **Добавить**.

2. В открывшемся окне **Создание точки назначения** в поле **Точка назначения** выберите тип точки назначения, которую вы хотите добавить, или создайте новую, нажав **Создать** и настроив следующие параметры:

   a. На вкладке **Основные параметры** в поле **Название** введите уникальное имя точки назначения. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   b. С помощью переключателя **Состояние** вы можете при необходимости включить или выключить сервис.

   c. В раскрывающемся списке **Тип** выберите тип точки назначения. Доступны следующие значения:

   - internal
   - nats-jetstream
   - tcp
   - udp
   - http
   - diode
   - kafka
   - file
   - storage
   - correlator
   - eventRouter

   d. На вкладке **Дополнительные параметры** укажите значения для параметров настройки. Набор параметров для настройки зависит от типа точки назначения, выбранного на вкладке **Основные параметры**. Более подробная информация о параметрах и значениях доступна по ссылке для каждого типа точки назначения в пункте c. этой инструкции.

Созданная точка назначения отобразится на вкладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

8 Проверка параметров коллектора

На этом этапе в Kaspersky SIEM Cloud создается набор ресурсов для сервиса и на основе этого набора автоматически создаются сервисы:

- Набор ресурсов для коллектора отображается в разделе **Мониторинг → Ресурсы и сервисы → Коллекторы**. Его можно использовать для создания новых сервисов коллектора. При изменении этого набора ресурсов все сервисы, которые работают на его основе, будут использовать новые параметры, если сервисы перезапустить: для этого можно использовать кнопки **Сохранить и перезапустить сервисы** и **Сохранить и обновить параметры сервисов**.

  Набор ресурсов можно изменять, копировать, переносить из папки в папку, удалять, импортировать и экспортировать, как другие ресурсы.

- Сервисы отображаются в разделе **Мониторинг → Ресурсы и сервисы → Активные сервисы**. Созданные с помощью мастера установки сервисы выполняют функции внутри решения Kaspersky SIEM Cloud – для связи с внешними частями сетевой инфраструктуры необходимо установить аналогичные внешние сервисы на предназначенных для них серверах и устройствах. Например, внешний сервис коллектора следует установить на сервере, предназначенном для получения событий; внешние сервисы хранилища – на серверах с развернутой службой ClickHouse; внешние сервисы агентов – на тех устройствах Windows, где требуется получать и откуда необходимо пересылать события Windows.

Чтобы проверить параметры коллектора:

1. В разделе **Проверка параметров** нажмите **Сохранить и создать сервис**.

   Отобразится таблица сервисов, созданных на основе набора ресурсов, выбранных в мастере установки. В нижней части окна отобразятся примеры команд, с помощью которых необходимо установить внешние аналоги этих сервисов на предназначенные для них серверы и устройства.

   Пример

   ```
   /opt/kaspersky/kuma/kuma collector --core https://kuma-example:<port used to communicate with the Kaspersky SIEM Cloud Core> --pair.fingerprint <Kaspersky SIEM Cloud Core CA certificate thumbprint ID> --id <service ID> --api.port <port used to communicate with the service> --install
   ```

   где:

   `<Kaspersky SIEM Cloud Core CA certificate thumbprint ID>` - идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса.

   Параметр `--pair.fingerprint` является необязательным. При создании сервиса Kaspersky SIEM Cloud автоматически добавляет этот параметр в команду установки и указывает идентификатор отпечатка. Вы можете выполнить установку сервиса без указания параметра `--pair.fingerprint`. В этом случае Kaspersky SIEM Cloud использует значение `insecure` по умолчанию, что не обеспечивает проверку подлинности CA-сертификата Ядра Kaspersky SIEM Cloud при установлении соединения. Если используется значение `insecure`, обновление отпечатка после перевыпуска CA-сертификата не требуется.

   Для обеспечения проверки подлинности CA-сертификата Ядра Kaspersky SIEM Cloud рекомендуется не удалять параметр `--pair.fingerprint` с идентификатором отпечатка при установке сервиса. При перевыпуске CA-сертификата необходимо скопировать новый отпечаток сертификата в веб-интерфейсе и перезапустить сервис с обновленным значением параметра.

   Файл `kuma` можно найти внутри установщика в директории `/kuma-ansible-installer/roles/kuma/files/`.

Порт для связи с Ядром Kaspersky SIEM Cloud, идентификатор сервиса, идентификатор отпечатка CA-сертификата и порт для связи с сервисом добавляются в команду автоматически. Также следует убедиться в сетевой связности системы Kaspersky SIEM Cloud и при необходимости открыть используемые ее компонентами порты.

2. Закройте окно создания коллектора, нажав **Сохранить коллектор**.

Сервис коллектора будет создан в Kaspersky SIEM Cloud. Теперь сервис необходимо установить на сервере, предназначенном для получения событий.

Если в коллекторе был выбран коннектор типа WEC, WMI или ETW, потребуется также установить автоматически созданные агенты Kaspersky SIEM Cloud.

После завершения создания и настройки коллектора требуется установить коллектор Kaspersky SIEM Cloud в облачной инфраструктуре или в локальной инфраструктуре.

Установка коллектора в локальной инфраструктуре

Облачные коллекторы не поддерживают передачу событий с помощью коннекторов типа **netflow**, **sflow**, **udp**, **snmp-trap**. Если вы планируете использование коннекторов этих типов для сбора событий, вам нужно установить коллектор в локальной инфраструктуре вашей организации. Локальный коллектор принимает события и отправляет их в облачную инфраструктуру для дальнейшей обработки и хранения.

Предварительные условия

Требования к серверу, на котором планируется установка коллектора:

- Сервер должен иметь доступ в интернет для доступа к облачной инфраструктуре.
- Сервер должен отвечать аппаратным и программным требованиям для установки локальных компонентов.
- На сервере должен быть установлен и отключен (режим **disabled**) SELinux.

Сценарий

Сценарий установки коллектора в локальной инфраструктуре состоит из следующих этапов:

❶ Создание в облачной инфраструктуре маршрутизатора событий

Используйте существующий или создайте новый маршрутизатор событий в облачной инфраструктуре. Поток событий от локального коллектора будет направлен в этот маршрутизатор событий.

❷ Создание коллектора в интерфейсе Kaspersky SIEM Cloud

Создайте и настройте локальный коллектор. На шаге **Маршрутизация** в качестве точки назначения укажите созданный маршрутизатор событий.

На шаге **Проверка параметров** вы можете скопировать и сохранить команду, которая потребуется вам при установке коллектора на сервере.

❸ Скачивание архива для установки коллектора в локальной инфраструктуре

После создания коллектора скачайте архив с файлами для установки коллектора на сервер.

> Скачать архив для установки коллектора может только пользователь с ролью Главный администратор или Администратор тенанта.

Чтобы скачать архив для установки коллектора:

1. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
2. На панели инструментов или в меню (⋮) выберите **Скачать архив для локального развертывания**.

Размер архива составляет около 0,5 ГБ. Процесс скачивания может занять до нескольких минут.

❹ Установка коллектора в локальной инфраструктуре

После создания коллектора необходимо установить его на сервере сетевой инфраструктуры, предназначенной для получения событий.

Чтобы установить коллектор в локальной инфраструктуре:

1. Войдите на сервер, на котором вы хотите установить сервис.
2. Создайте папку /opt/kaspersky/kuma/.
3. Скопируйте файл "kuma" в папку /opt/kaspersky/kuma/. Файл находится в архиве, который вы скачали после создания коллектора в интерфейсе Kaspersky SIEM Cloud.

   Убедитесь, что файл kuma имеет достаточные права для запуска. Если файл не является исполняемым, измените права для запуска с помощью следующей команды:

   ```
   sudo chmod +x /opt/kaspersky/kuma/kuma
   ```

4. Поместите в директорию /opt/kaspersky/kuma/ файл LICENSE. Файл находится в архиве, который вы скачали после создания коллектора в интерфейсе Kaspersky SIEM Cloud. Примите условия Лицензионного соглашения, выполнив следующую команду:

   ```
   sudo /opt/kaspersky/kuma/kuma license
   ```

5. Создайте пользователя kuma:

```
sudo useradd --system kuma && usermod -s /usr/bin/false kuma
```

6. Выдайте пользователю kuma права на директорию /opt/kaspersky/kuma и все файлы внутри директории:

```
sudo chown -R kuma:kuma /opt/kaspersky/kuma/
```

7. Получите идентификатор коллектора. Для этого в веб-интерфейсе в разделе **Мониторинг → Ресурсы и сервисы → Активные сервисы** откройте контекстное меню созданного коллектора и нажмите **Копировать идентификатор**.

8. Выполните следующую команду:

```
sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id
<service_ID> --api.port <API_port>
```

где:

- <FQDN> — полное доменное имя сервера Ядра Kaspersky SIEM Cloud.
- <port> — номер порта Ядра Kaspersky SIEM Cloud для внутренних коммуникаций (по умолчанию используется порт 7210).
- <CA_cert_ID> — идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса.

  Параметр `--pair.fingerprint` является необязательным. При создании сервиса Kaspersky SIEM Cloud автоматически добавляет этот параметр в команду установки и указывает идентификатор отпечатка.
  Вы можете выполнить установку сервиса без указания параметра `--pair.fingerprint`. В этом случае Kaspersky SIEM Cloud использует значение `insecure` по умолчанию, что не обеспечивает проверку подлинности CA-сертификата Ядра Kaspersky SIEM Cloud при установлении соединения. Если используется значение `insecure`, обновление отпечатка после перевыпуска CA-сертификата не требуется.

  Если вы хотите указать идентификатор отпечатка для обеспечения проверки подлинности CA-сертификата Ядра Kaspersky SIEM Cloud, перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**, установите флажок рядом с сервисом Ядра Kaspersky SIEM Cloud, в меню (⋮) выберите **Копировать отпечаток сертификата**, затем скопированный идентификатор используйте в команде установки коллектора.

  Для обеспечения проверки подлинности CA-сертификата Ядра Kaspersky SIEM Cloud рекомендуется не удалять параметр `--pair.fingerprint` с идентификатором отпечатка при установке сервиса. При перевыпуске CA-сертификата необходимо скопировать новый отпечаток сертификата в веб-интерфейсе и перезапустить сервис с обновленным значением параметра.

- <service_ID> — идентификатор сервиса, скопированный из веб-интерфейса Kaspersky SIEM Cloud.
- <API_port> — порт, используемый для связи с устанавливаемым компонентом.

Пример

```
sudo /opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXX
--api.port YYYY
```

Если в результате выполнения команды были выявлены ошибки, проверьте корректность параметров. Например, наличие требуемого уровня доступа, сетевой доступности между сервисом коллектора и Ядром, уникальность выбранного API-порта. После устранения ошибок продолжите установку коллектора.

Если ошибки не выявлены, а статус коллектора в веб-интерфейсе Kaspersky SIEM Cloud изменился на *зеленый*, остановите выполнение команды и перейдите к следующему шагу.

Команду можно скопировать на последнем шаге мастера установщика. В команде автоматически указывается адрес и порт сервера Ядра Kaspersky SIEM Cloud, идентификатор устанавливаемого коллектора, идентификатор отпечатка CA-сертификата, а также порт, который этот коллектор использует для связи.

При развертывании нескольких сервисов Kaspersky SIEM Cloud на одном хосте в процессе установки необходимо указать уникальные порты для каждого компонента с помощью параметра `--api.port <API_port>`. По умолчанию используется значение `--api.port 7221`.

Перед установкой вам нужно убедиться в сетевой связности компонентов Kaspersky SIEM Cloud.

9. Выполните команду повторно, добавив ключ `--install`:

```
sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id <service_ID> --api.port <API_port> --install
```

Пример

```
sudo /opt/kaspersky/kuma/kuma collector --core https://example.com:7210 --pair.fingerprint XXXX --id XXXX --api.port YYYY --install
```

10. Добавьте порт коллектора Kaspersky SIEM Cloud в исключения брандмауэра.

Для правильной работы решения убедитесь, что компоненты Kaspersky SIEM Cloud могут взаимодействовать с другими компонентами и программами по сети через протоколы и порты, указанные во время установки компонентов Kaspersky SIEM Cloud.

Коллектор установлен. С его помощью можно получать и передавать на обработку данные из источника события.

11. В разделе **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы** убедитесь, что у установленного вами коллектора зеленый статус.

Если статус коллектора отличается от зеленого, просмотрите журнал этого сервиса на машине, где он установлен, в директории `/opt/kaspersky/kuma/collector/<идентификатор коллектора>/log/collector`. Ошибки записываются в журнал вне зависимости от того, включен или выключен режим отладки.

Если коллектор установлен правильно и вы уверены, что из источника событий приходят данные, то при поиске связанных с ним событий в таблице должны отображаться события.

Если требуется, проверьте список портов, необходимых для работы локального коллектора.

Чтобы проверить наличие ошибок нормализации с помощью раздела События веб-интерфейса Kaspersky SIEM Cloud:

1. Убедитесь, что запущен сервис коллектора.
2. Убедитесь, что источник событий передает события в Kaspersky SIEM Cloud.
3. Убедитесь, что в разделе **Ресурсы** веб-интерфейса Kaspersky SIEM Cloud в раскрывающемся списке **Хранить исходное событие** ресурса **Нормализатор** выбрано значение **При возникновении ошибок**.
4. В разделе **События** в Kaspersky SIEM Cloud выполните поиск событий со следующими параметрами:

```
ServiceID = <ID of the collector to check>
Raw != ""
```

Если при этом поиске будут обнаружены какие-либо события, это означает, что есть ошибки нормализации, и их необходимо исследовать.

Чтобы проверить наличие ошибок нормализации с помощью панели мониторинга Kaspersky SIEM Cloud Collectors:

1. Убедитесь, что запущен сервис коллектора.
2. Убедитесь, что источник событий передает события в Kaspersky SIEM Cloud.
3. Откройте раздел **Метрики** и перейдите по ссылке **Kaspersky SIEM Cloud Collectors**.
4. Проверьте, отображаются ли ошибки в разделе **Errors (Ошибки)** виджета **Normalization (Нормализация)**.

Если в результате обнаружены ошибки нормализации, их необходимо исследовать.

В коллекторах, которые используют в качестве транспорта коннекторы типа WEC, WMI или ETW, необходимо убедиться, что для подключения к агенту используется уникальный порт. Этот порт указывается в разделе **Транспорт** при создании коллектора.

Обогащение событий данными Kaspersky CyberTrace

В Kaspersky SIEM Cloud поддерживается потоковое обогащение событий данными Kaspersky CyberTrace (далее CyberTrace), включая информацию об индикаторах компрометации (IoC). Обогащение выполняется в инфраструктуре пользователя, где развернут сервер CyberTrace, а затем обогащенные события передаются в облачную инфраструктуру для корреляции и хранения.

В статье описан пример настройки решения для получения событий с межсетевого экрана и прокси-сервера.

Предусловия

- Решение Kaspersky SIEM Cloud активировано.
- В инфраструктуре пользователя развернут сервер CyberTrace.

- У вас достаточно доступных вычислительных единиц для развертывания маршрутизатора событий.
- В инфраструктуре пользователя есть аппаратные мощности для развертывания коллекторов.

Этапы

Настройка обогащения событий данными CyberTrace состоит из следующих этапов:

1. **Создание точек назначения для хранилища и коррелятора**

   Если у вас еще не созданы точки назначения типа **storage** и **correlator** для хранилища и коррелятора в облачной инфраструктуре, создайте их. В параметрах точек назначения укажите URL хранилища и URL коррелятора.

2. **Создание и настройка маршрутизатора событий**

   Создайте и разверните в облачной инфраструктуре маршрутизатор событий. На этот маршрутизатор будут направлены потоки событий с коллекторов, установленных в локальной инфраструктуре.

   В разделе **Маршрутизация** добавьте точки назначения типа **storage** и **correlator** для хранилища и коррелятора.

3. **Создание точки назначения для маршрутизатора событий**

   Создайте точку назначения типа **eventRouter**. В параметрах точки назначения укажите URL маршрутизатора событий.

4. **Создание и настройка коллекторов в локальной инфраструктуре**

   Для каждого источника событий (межсетевой экран и прокси-сервер) создайте локальный коллектор. В свойствах коллекторов в разделе **Маршрутизация** укажите созданную точку назначения для маршрутизатора событий.

   Для настройки обогащения укажите в каждом коллекторе следующие параметры:

   - В качестве транспорта выберите любой коннектор (например, **http**).
   - В качестве метода нормализации выберите любой метод (например, **json**) с сопоставлением следующих полей: `SourceHostName`, `DestinationHostName`, `Message`, `DeviceHostName`, `DeviceAddress`, `FileHash`, `OldFileHash`, `RequestUrl`.
   - В качестве обогащения создайте правило обогащения событий, в котором тип источника данных – **cybertrace-http**, указана версия CyberTrace **≥ 5.0**, и в раскрывающемся списке **Ключевые поля** выбраны следующие поля нормализатора: `SourceHostName`, `DestinationHostName`, `Message`, `DeviceHostName`, `DeviceAddress`, `FileHash`, `OldFileHash`, `RequestUrl`.

События с сетевого экрана и прокси-сервера будут обогащаться и отправляться в облачную инфраструктуру.

Обеспечение бесперебойной работы коллекторов

Бесперебойное поступление событий от источника событий в Kaspersky SIEM Cloud является важным условием защиты сетевой инфраструктуры.

Настройка бесперебойности поступления событий состоит из следующих этапов:

1 Установка коллектора

На стороне Kaspersky SIEM Cloud установите два или больше одинаковых коллекторов.

2 Настройка управления потоками событий между коллекторами

На стороне источника событий настройте управление потоками событий между коллекторами с помощью сторонних средств управления нагрузкой серверов.

1. Если вы хотите управлять потоком событий с помощью rsyslog, выполните следующие действия:

   a. Установите на сервере источника событий rsyslog (см. документацию rsyslog).

   b. Добавьте в конфигурационный файл `/etc/rsyslog.conf` правила перенаправления потока событий между коллекторами:

   ```
   *.* @@<FQDN of the primary collector server>:<port on which the collector receives events>
   $ActionExecOnlyWhenPreviousIsSuspended on
   & @@<FQDN of the standby collector server>:<port on which the collector receives events>
   $ActionExecOnlyWhenPreviousIsSuspended off
   ```

   Пример конфигурационного файла

   Пример конфигурационного файла, где указан один основной коллектор и два резервных. Коллекторы настроены на принятие событий на порт TCP 5140.

   ```
   *.* @@kuma-collector-01.example.com:5140
   $ActionExecOnlyWhenPreviousIsSuspended on
   & @@kuma-collector-02.example.com:5140
   & @@kuma-collector-03.example.com:5140
   $ActionExecOnlyWhenPreviousIsSuspended off
   ```

   c. Перезапустите rsyslog с помощью команды:

   ```
   systemctl restart rsyslog
   ```

2. Если вы хотите управлять потоком событий с помощью nginx, выполните следующие действия:

   a. Установите nginx на сервере, предназначенном для управления потоком событий, с помощью одной из следующих команд:

   - Команда для установки в Oracle Linux 8.6:

     ```
     $sudo dnf install nginx
     ```

- Команда для установки в Ubuntu 20.4:

```
$sudo apt-get install nginx
```

При установке из sources, необходимо собрать с параметром `-with-stream`:
`$sudo ./configure -with-stream -without-http_rewrite_module -without-http_gzip_module`

b. На nginx-сервере в конфигурационный файл `nginx.conf` добавьте модуль `stream` с правилами перенаправления потока событий между коллекторами.

Пример модуля stream

Пример модуля, в котором поток событий распределяется между коллекторами kuma-collector-01.example.com и kuma-collector-02.example.com, которые принимают события по протоколу TCP на порт 5140 и по протоколу UDP на порт 5141. Для балансировки используется ngnix-сервер nginx.example.com.

```
stream {
 upstream syslog_tcp {
server kuma-collector-1.example.com:5140;
server kuma-collector-2.example.com:5140;
}
upstream syslog_udp {
server kuma-collector-1.example.com:5141;
server kuma-collector-2.example.com:5141;
}
 server {
listen nginx.example.com:5140;
proxy_pass syslog_tcp;
}
server {
listen nginx.example.com:5141 udp;
proxy_pass syslog_udp;
proxy_responses 0;
}
}
 worker_rlimit_nofile 1000000;
events {
worker_connections 20000;
}
# worker_rlimit_nofile – ограничение на максимальное число открытых файлов (RLIMIT_NOFILE) для рабочих процессов. Используется для увеличения ограничения без перезапуска главного процесса.
# worker_connections – максимальное число соединений, которые одновременно может открыть рабочий процесс.
```

При большом количестве активных сервисов и пользователей может понадобиться увеличить лимит открытых файлов в параметрах `nginx.conf`.

Пример

```
worker_rlimit_nofile 1000000;
events {
worker_connections 20000;
}
```

где:

- `worker_rlimit_nofile` – ограничение на максимальное число открытых файлов (RLIMIT_NOFILE) для рабочих процессов. Используется для увеличения ограничения без перезапуска главного процесса;
- `worker_connections` – максимальное число соединений, которые одновременно может открыть рабочий процесс.

c. Перезапустите nginx, выполнив команду:

```
systemctl restart nginx
```

d. На сервере источника событий перенаправьте события на nginx-сервер.

Для тонкой настройки балансировки может потребоваться nginx Plus, однако некоторые методы балансировки, например Round Robin и Least Connections, доступны в базовой версии ngnix.

> Подробнее о настройке nginx см. в документации nginx.

При такой конфигурации коллекторов поступающие события не будут теряться, когда сервер коллектора по какой-либо причине недоступен.

Необходимо учитывать, что при переключении потока событий между коллекторами агрегация событий будет происходить на каждом коллекторе отдельно.

3 Исправление ошибок (при необходимости)

Если коллектор Kaspersky SIEM Cloud не удается запустить, а в его журнале выявлена ошибка `"panic: runtime error: slice bounds out of range [8:0]"`, выполните следующие действия:

1. Остановите коллектор, с помощью команды:

```
sudo systemctl stop kuma-collector-<collector ID>
```

2. Удалите файлы с кешем DNS-обогащения.

```
sudo rm -rf /opt/kaspersky/kuma/collector/<collector ID>/cache/enrichment/DNS-*
```

3. Удалите файлы с кешем событий (дисковый буфер). Выполняйте команду, только если можно пожертвовать событиями, находящимися в дисковых буферах коллектора.

```
sudo rm -rf /opt/kaspersky/kuma/collector/<collector ID>/buffers/*
```

4. Запустите сервис коллектора.

```
sudo systemctl start kuma-collector-<collector ID>
```

Агрегирование событий

Правила агрегации позволяют объединить однотипные повторяющиеся события и заменить их одним общим событием. В правилах агрегации поддерживается работа с полями стандартной схемы событий Kaspersky SIEM Cloud и с полями расширенной схемы событий. Таким образом, вы можете уменьшить количество схожих событий, передаваемых в хранилище и/или коррелятор, снизить нагрузку на сервисы, сэкономить место для хранения данных и сэкономить лицензионную квоту (EPS). Агрегационное событие создается по достижении порога по времени или порога по количеству событий, в зависимости от того, что произойдет раньше.

Для правил агрегации можно настроить фильтр и применять его только к событиям, которые соответствуют заданным условиям.

В поставку Kaspersky SIEM Cloud включено правило агрегации [OOTB] Netflow 9. Правило сработает при достижении 100 событий или по истечении 10 секунд.

Агрегация событий выполняется по следующим полям:

- `DestinationAddress`
- `DestinationPort`
- `SourceAddress`
- `TransportProtocol`
- `DeviceVendor`
- `DeviceProduct`

Поля `DeviceCustomString1` и `BytesIn` суммируются.

Чтобы создать правило агрегации:

1. В веб-интерфейсе перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Правила агрегации** и нажмите кнопку **Создать**.

2. В поле **Название** введите название для создаваемого правила агрегации. Название должно содержать от 1 до 128 символов в кодировке Unicode.

3. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит правило агрегации.

4. В поле **Предел событий** укажите количество событий, которое должно быть получено, чтобы сработало правило агрегации и события были объединены. Значение по умолчанию: `100`.

5. В поле **Время ожидания событий** укажите количество секунд, в течение которых коллектор получает события для объединения. По истечении этого срока правило агрегации срабатывает и создается новое агрегационное событие. Значение по умолчанию: `60`.

6. В поле **Описание** введите описание правила агрегации. Максимальная длина описания: 4000 символов в кодировке Unicode.

7. В поле **Группирующие поля** с помощью кнопки **Добавить поле** выберите поля, по которым будут определяться однотипные события. Вы можете выбрать следующие служебные поля: SourceAssetID, DestinationAssetID, DeviceAssetID, SourceAccountID, DestinationAccountID. Идентификаторы активов добавляются после нормализации события, поэтому по ним можно будет агрегировать события. Остальные служебные поля не используются в агрегации. Выбранные события можно удалять с помощью кнопок со значком крестика.

8. В поле **Уникальные поля** с помощью кнопки **Добавить поле** можно выбрать поля, при наличии которых коллектор исключит событие из процесса агрегации даже при наличии полей, указанных в разделе **Группирующие поля**. Выбранные события можно удалять с помощью кнопок со значком крестика.

   Если в **Уникальные поля** вы укажете более одного поля, то уникальными должны быть сочетания значений всех этих полей.

   Уникальные поля не сохраняются в агрегированном событии.

9. В поле **Поля суммы** с помощью кнопки **Добавить поле** можно выбрать поля, значения которых будут просуммированы в процессе агрегации. Выбранные события можно удалять с помощью кнопок со значком крестика.

   Существуют следующие особенности поведения полей:

   - значения полей с типами `Число` и `Число с плавающей точкой` суммируются;
   - значения полей с типом `Строка` конкатенируются через запятую;
   - значения полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` добавляются в конец массива.

10. В блоке параметров **Параметры фильтра** задайте условия определения событий, которые будут обрабатываться этим правилом. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр.

    Как создать фильтр в ресурсах ?

    Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

    Чтобы создать фильтр:

    1. В раскрывающемся списке **Фильтр** выберите **Создать**.
    2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят.
    3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.
    4. Выберите режим создания фильтра: **Конструктор** или **Код**.

       При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра.

5. Если вы выбрали вариант **Конструктор**, выполните следующие действия:

a. В раскрывающемся списке выберите логический оператор:

- **И** – отбирает события, которые соответствуют всем указанным условиям.
- **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий.
- **НЕ** – отбирает события, которые не соответствуют всем указанным условиям.

b. Нажмите на кнопку **Добавить условие**.

c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра.

Операнды фильтров

- **Поля событий** – поле события, которое требуется использовать как операнд фильтра.
- **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**.

  Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра.
- **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры:
  - **словарь** (обязательно) – словарь, который требуется использовать.
  - **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.
- **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события.
  - **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать.
  - **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы.
  - **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда.
  - **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда.

- **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
  - **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**.
  - **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.
- **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
  - **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
  - **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
  - **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
- **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
  - **значение** (обязательно) – константа, которую требуется присвоить операнду.
- **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
  - **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.

Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в коррелляторах.

- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.

Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.

e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.

Вы можете добавить несколько групп условий.

6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.

   В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕.

8. Нажмите **Сохранить**.

Не используйте в правилах агрегации фильтры с операндом **TI** или операторами **TIDetect**, **inActiveDirectoryGroup** и **hasVulnerability**. Поля `Active Directory`, для которых используется оператор **inActiveDirectoryGroup,** появляются на этапе обогащения, то есть после выполнения правил агрегации.

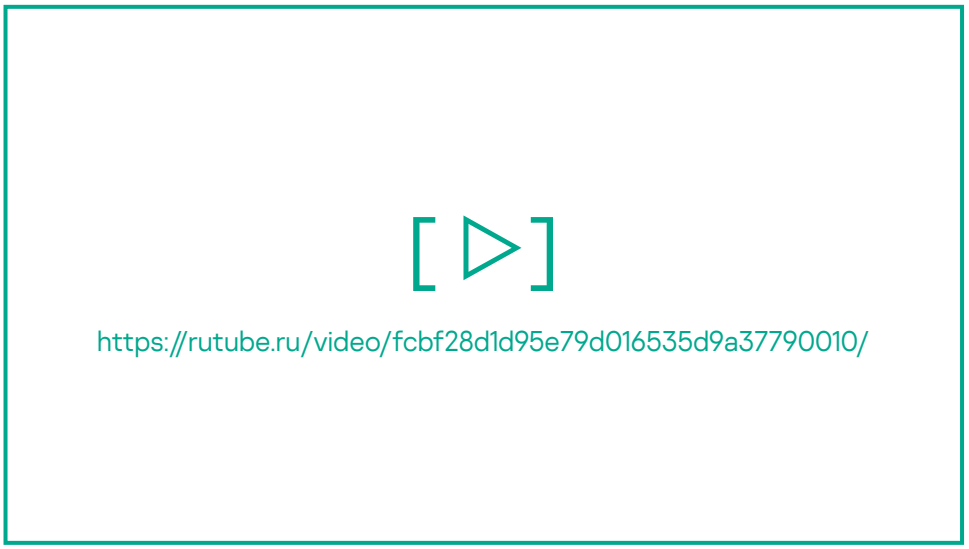
11. Нажмите кнопку **Создать**.

После создания правила агрегации вы можете привязать его коллектору.

Нормализация событий

Нормализаторы предназначены для приведения исходных событий, которые поступают из разных источников в разных форматах, к модели данных событий Kaspersky SIEM Cloud. Нормализованные события становятся доступны для обработки другими ресурсами и сервисами Kaspersky SIEM Cloud.

Для наглядного ознакомления с нормализаторами вы можете просмотреть видео ниже.



https://rutube.ru/video/fcbf28d1d95e79d016535d9a37790010/

Нормализатор состоит из *основного* и необязательных *дополнительных правил парсинга событий*. С помощью создания основного и множества дополнительных правил парсинга можно реализовать сложную логику обработки событий. Данные передаются по древовидной структуре правил парсинга в зависимости от условий, заданных в параметре

Условия дополнительной нормализации. Последовательность создания правил парсинга имеет значение: событие обрабатывается последовательно и последовательность обработки обозначена стрелками. Нормализация событий доступна в следующих вариантах:

- 1 коллектор – 1 нормализатор.

  Мы рекомендуем использовать такой способ, если у вас много событий одного типа или много IP-адресов, откуда могут приходить события одного типа. Можно настроить один коллектор только с одним нормализатором и это будет оптимально с точки зрения производительности.

- 1 коллектор – несколько нормализаторов с привязкой к IP-адресу.

  Такой способ доступен для коллекторов с коннектором типа UDP, TCP, HTTP. Если в коллекторе на шаге Транспорт указан коннектор UDP, TCP, HTTP, на шаге Парсинг событий на вкладке Настройки парсинга вы можете задать несколько IP-адресов и указать, какой нормализатор использовать для событий, поступающих с заданных адресов. Доступны следующие типы нормализаторов: json, cef, regexp, syslog, csv, kv, xml. Для нормализаторов типа Syslog и regexp вы можете задать дополнительные условия нормализации в зависимости от значения поля DeviceProcessName.

Чтобы создать нормализатор:

1. В веб-интерфейсе перейдите в раздел **Мониторинг → Ресурсы и сервисы → Нормализаторы** и нажмите кнопку **Создать.**

2. В поле **Название** введите уникальное имя нормализатора. Максимальная длина имени: до 128 символов в кодировке Unicode.

3. В раскрывающемся списке **Тенант**, которому принадлежит нормализатор.

4. В раскрывающемся списке **Метод парсинга** выберите тип получаемых событий. В зависимости от выбранного значения вы можете использовать преднастроенные правила сопоставления полей событий или указать правила вручную. При выборе определенных методов парсинга могут стать доступны дополнительные параметры, для которых вам нужно указать значения.

   Доступные методы парсинга:

   json

   Этот метод парсинга используется для обработки данных в формате JSON, в которых каждый объект, включая его вложенные объекты, занимает одну строку файла.

   При обработке файлов с иерархически выстроенными данными вы можете обращаться к полям вложенных объектов, указывая названия параметров поочередно через точку. Например, к параметру `username` из строки `"user":{"username":"system:node:example-01"}` можно обратиться с помощью запроса `user.username`.

   Файлы обрабатываются построчно. Многострочные объекты с вложенными структурами могут быть нормализованы неправильно.

   В сложных схемах нормализации, где используются дополнительные нормализаторы, все вложенные объекты обрабатываются на первом уровне нормализации за исключением случаев, когда условия дополнительной нормализации не заданы и обрабатываемое событие целиком передается в дополнительный нормализатор.

   В качестве разделителя строк вы можете использовать символы `\n` и `\r\n`. Строки должны быть в кодировке UTF-8.

   Если вы хотите передавать сырое событие для дополнительной нормализации, на каждом уровне вложенности в окне **Дополнительный парсинг события** в раскрывающемся списке **Использовать сырое событие** выберите **Да**.

   cef

   Этот метод парсинга используется для обработки данных в формате CEF.

   При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат Kaspersky SIEM Cloud, нажав на кнопку **Применить сопоставление по умолчанию**.

   regexp

   Этот метод парсинга используется для создания собственных правил обработки данных в формате с использованием регулярных выражений.

   Вам нужно добавить регулярное выражение (синтаксис RE2) с именованными группами захвата в поле блока параметров **Нормализация**. Имя группы захвата и ее значение будут считаться полем и значением сырого события, которое можно будет преобразовать в поле события формата Kaspersky SIEM Cloud.

Чтобы добавить правила обработки событий:

1. При необходимости в поле **Примеры событий** скопируйте пример данных, которые вы хотите обработать. Мы рекомендуем выполнить этот шаг.

   Вы также можете сгенерировать регулярные выражения на основе добавленных примеров по кнопке **Сгенерировать регулярное выражение с помощью KIRA**. В этом случае сгенерированные регулярные выражения автоматически добавятся в блок параметров **Нормализация**.

2. В поле блока параметров **Нормализация** добавьте регулярное выражение с именованными группами захвата в синтаксисе RE2, например `"(?P<name>regexp)"`. Регулярное выражение, добавленное в поле блока параметров **Нормализация**, должно полностью совпадать с событием. При разработке регулярного выражения рекомендуется использовать специальные символы, обозначающие начало и конец текста: `^`, `$`.

   Вы можете добавить несколько регулярных выражений или удалить регулярные выражения. Для добавления регулярного выражения нажмите на кнопку **Добавить регулярное выражение**. Для удаления регулярного выражения нажмите рядом с ним на значок удаления ✕.

3. Нажмите на кнопку **Перенести названия полей в таблицу**.

   Имена групп захвата отображаются в столбце **Поле KUMA** таблицы **Сопоставление**. Вы можете выбрать соответствующее группе захвата поле Kaspersky SIEM Cloud в столбце напротив каждой группы захвата. Если вы именовали группы захвата в соответствии с форматом CEF, вы можете использовать автоматическое сопоставление CEF, установив флажок **Использовать синтаксис CEF при нормализации**.

Правила обработки событий будут добавлены.

syslog

Этот метод парсинга используется для обработки данных в формате syslog.

При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат Kaspersky SIEM Cloud, нажав на кнопку **Применить сопоставление по умолчанию**.

Для парсинга событий в формате rfc5424 с секцией `structured-data` вам нужно в раскрывающемся списке **Сохранить дополнительные поля** выбрать **Да**. В этом случае значения из секции `structured-data` станут доступны в полях `Extra`.

csv

Этот метод парсинга используется для создания собственных правил обработки данных в формате CSV.

При выборе этого метода парсинга вам нужно в поле **Разделитель** указать разделитель значений в строке. В качестве разделителя значений в строке можно использовать любой однобайтовый символ ASCII.

kv

Этот метод парсинга используется для обработки данных в формате ключ-значение. Доступные параметры метода парсинга описаны в таблице ниже.

Доступные параметры метода парсинга

Параметр	Описание
Разделитель пар	Символ для разделения пар ключ-значение. Вы можете указать любое односимвольное (1 байт) значение. Указанное значение не должно совпадать со значением, указанным в поле **Разделитель значений**.
Разделитель значений	Символ для разделения ключа и значения. Вы можете указать любое односимвольное (1 байт) значение. Указанное значение не должно совпадать со значением, указанным в поле **Разделитель пар**.

xml

Этот метод парсинга используется для обработки данных в формате XML, в которых каждый объект, включая вложенные объекты, занимает одну строку файла. Файлы обрабатываются построчно.

Если вы хотите передавать сырое событие для дополнительной нормализации, на каждом уровне вложенности в окне **Дополнительный парсинг события** в раскрывающемся списке **Использовать сырое событие** выберите **Да**.

При выборе этого метода парсинга вы можете указать ключевые атрибуты XML, которые требуется извлекать из тегов, в блоке параметров **Атрибуты XML**. Если в структуре XML в одном теге есть атрибуты XML с разными значениями, вы можете определить значение, указав ключ к значению в столбце **Исходные данные** таблицы **Сопоставление**.

Чтобы добавить ключевые атрибуты XML:

1. Нажмите на кнопку **+ Добавить поле**.

2. В открывшемся окне укажите путь к атрибуту XML.

Вы можете добавить несколько атрибутов XML и удалить атрибуты XML. Для удаления отдельного атрибута XML нажмите рядом с ним на значок удаления ✕. Для удаления всех атрибутов XML нажмите на кнопку **Сбросить**.

Если ключевые атрибуты XML не указаны, при сопоставлении полей уникальный путь к значению XML будет представлен последовательностью тегов.

Нумерация тегов

В Kaspersky SIEM Cloud доступна автоматическая нумерация тегов в событиях в формате XML. Это позволяет распарсить событие с одинаковыми тегами или неименованными тегами, такими как `<Data>`.

В качестве примера мы используем нумерацию тегов атрибута `EventData` события Microsoft Windows PowerShell event ID 800.

Посмотреть события Microsoft Windows PowerShell event ID 800

```
<Event xmlns="http://schemas .microsoft.com/win/2004/08/events/event">
        <System>
                <Provider Name="Microsoft-Windows-ActiveDirectory_DomainService" Guid="{0e8478c5-3605-4e8c-
8497-1e730c959516}" EventSourceName="NTDS" />
                <EventID Qualifiers="0000">0000</EventID>
                <Version>@</Version>
                <Level>4</Level>
                <Task>15</Task>
                <Opcode>0</Opcode>
                <Keywords >0x8080000000000000</Keywords>
                <TimeCreated SystemTime="2000-01-01T00:00:00.6594959002" />
                <EventRecordID>55647</EventRecordID>
                <Correlation />
                <Execution ProcessID="1" ThreadID="1" />
                <Channel>service</Channel>
                <Computer>computer</Computer>
                <Security UserID="0000" />
        </System>
        <EventData>
                <Data>583</Data>
                <Data>36</Data>
                <Data>192.168.0.1:5084</Data>
                <Data>level</Data>
```

```
                <Data>name, lDAPDisplayName</Data>
                <Data />
                <Data>5545</Data>
                <Data>3</Data>
                <Data>0</Data>
                <Data>0</Data>
                <Data>0</Data>
                <Data>15</Data>
                <Data>none</Data>
        </EventData>
</Event>
```

Для парсинга событий с одинаковыми тегами или неименованными тегами вам нужно настроить нумерацию тегов и маппинг данных для пронумерованных тегов с полями события Kaspersky SIEM Cloud.

Kaspersky SIEM Cloud поддерживает одновременное использование атрибутов XML и нумерации тегов в рамках одного экстранормализатора. Если атрибут XML содержит неименованные теги или одинаковые теги, мы рекомендуем использовать нумерацию тегов. Если атрибут XML содержит только именованные теги, мы рекомендуем использовать атрибуты XML.

Для использования атрибутов XML и нумерации тегов в экстранормализаторах вам нужно последовательно включить параметр **Использовать сырое событие** в каждом экстранормализаторе по пути следования события в целевой экстранормализатор и в целевом экстранормализаторе.

В качестве примера работы нумерации тегов вы можете обратиться к нормализатору **MicrosoftProducts**. Параметр **Использовать сырое событие** включен последовательно в экстранормализаторах **AD FS** и **424**.

Чтобы настроить парсинг событий с неименованными или одинаковыми тегами:

1. Откройте существующий или создайте новый нормализатор.

2. В окне нормализатора **Основной парсинг событий** в раскрывающемся списке **Метод парсинга** выберите **xml**.

3. В поле **Нумерация тегов** нажмите на кнопку **+ Добавить поле**.

4. В отобразившемся поле укажите полный путь к тегу, элементам которого требуется присвоить порядковый номер, например `Event.EventData.Data`. Первому тегу будет присвоен номер 0. Если тег пустой, например `<Data />`, ему также будет присвоен порядковый номер.

5. Для настройки маппинга данных в группе параметров **Сопоставление** нажмите на кнопку **+ Добавить строку** и выполните следующие действия:

   a. В отобразившейся строке в поле **Исходные данные** укажите полный путь к тегу и индекс тега. Например, для события Microsoft Windows PowerShell event ID 800 из примера выше полные пути к тегам и индексы тегов будут выглядеть следующим образом:

      - `Event.EventData.Data.0`
      - `Event.EventData.Data.1`
      - `Event.EventData.Data.2`

   b. В раскрывающемся списке **Поле KUMA** выберите поле в событии Kaspersky SIEM Cloud, в которое попадет значение из пронумерованного тега после выполнения парсинга.

6. Сохраните изменения одним из следующих способов:

   - Если вы создали новый нормализатор, нажмите на кнопку **Сохранить**.
   - Если вы изменили существующий нормализатор, в коллекторе, к которому привязан нормализатор, нажмите на кнопку **Обновить параметры**.

Настройка парсинга будет завершена.

netflow

Этот метод парсинга используется для обработки данных во всех поддерживаемых форматах на основе протокола NetFlow: NetFlow v5, NetFlow v9 и IPFIX.

При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат Kaspersky SIEM Cloud, нажав на кнопку **Применить сопоставление по умолчанию**. При этом будут учтены исходные поля всех версий NetFlow (NetFlow v5, NetFlow v9 и IPFIX).

Если метод парсинга **netflow** выбран для основного парсинга, дополнительная нормализация недоступна.

В правилах сопоставления по умолчанию для метода парсинга **netflow** в полях событий Kaspersky SIEM Cloud не указывается тип протокола. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** вам нужно создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

netflow5

Этот метод парсинга используется для обработки данных в формате NetFlow v5.

При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат Kaspersky SIEM Cloud, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **netflow5** выбран для основного парсинга, дополнительная нормализация недоступна.

В правилах сопоставления по умолчанию для метода парсинга **netflow5** в полях событий Kaspersky SIEM Cloud не указывается тип протокола. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** вам нужно создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

netflow9

Этот метод парсинга используется для обработки данных в формате NetFlow v9.

При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат Kaspersky SIEM Cloud, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **netflow9** выбран для основного парсинга, дополнительная нормализация недоступна.

В правилах сопоставления по умолчанию для метода парсинга **netflow9** в полях событий Kaspersky SIEM Cloud не указывается тип протокола. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** вам нужно создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

sflow5

Этот метод парсинга используется для обработки данных в формате sflow5.

При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат Kaspersky SIEM Cloud, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **sflow5** выбран для основного парсинга, дополнительная нормализация недоступна.

ipfix

Этот метод парсинга используется для обработки данных в формате IPFIX.

При выборе этого метода парсинга вы можете использовать преднастроенные правила преобразования событий в формат Kaspersky SIEM Cloud, нажав на кнопку **Применить сопоставление по умолчанию**. Если метод парсинга **ipfix** выбран для основного парсинга, дополнительная нормализация недоступна.

> В правилах сопоставления по умолчанию для метода парсинга **ipfix** в полях событий Kaspersky SIEM Cloud не указывается тип протокола. При парсинге данных в формате NetFlow на вкладке нормализатора **Обогащение** вам нужно создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

sql

Нормализатор использует этот метод парсинга для обработки данных, полученных с помощью выборки из базы данных.

normalizer

Этот метод парсинга позволяет переиспользовать ранее созданный нормализатор в качестве основного или дополнительного для обработки событий.

При выборе этого метода парсинга вам нужно в раскрывающемся списке **Нормализатор** выбрать один из ранее созданных нормализаторов с типом json, cef, regexp, syslog, csv, kv, xml или sql. Нормализаторы с методом парсинга **normalizer** недоступны для выбора.

5. В раскрывающемся списке **Теги** выберите теги для нормализатора.

6. В раскрывающемся списке **Сохранить исходное событие** выберите, требуется ли сохранять исходное сырое событие в повторно созданном нормализованном событии:

   - **Не сохранять** – не сохранять исходное событие. Это значение выбрано по умолчанию.
   - **При возникновении ошибок** – сохранять исходное событие в поле `Raw` нормализованного события, если в процессе парсинга возникли ошибки. Вы можете использовать это значение при отладке сервиса. В этом случае появление у событий непустого поля `Raw` будет являться признаком неполадок.
   - **Всегда** – сохранять сырое событие в поле `Raw` нормализованного события.

7. В раскрывающемся списке **Сохранить дополнительные поля** выберите, требуется ли сохранять поля исходного события в нормализованном событии, если для них не было настроено сопоставление (см. шаг 8 этой инструкции):

   - **Нет**. Это значение выбрано по умолчанию.
   - **Да**. Поля исходного события сохраняются в поле `Extra` нормализованного события.

   Это поле недоступно, если в поле **Метод парсинга** выбрано значение **normalizer**.

8. При необходимости в поле **Примеры событий** укажите пример данных, которые вы хотите обработать. Мы рекомендуем выполнить этот шаг.

   Это поле недоступно, если в поле **Метод парсинга** выбрано значение **normalizer**.

   Вы можете добавить несколько примеров событий. Каждый новый пример нужно указывать с новой строки. При этом в таблице **Сопоставление** его результат парсинга отобразится в столбце **Примеры**. Это позволяет проверить правильность сопоставления полей для разных типов входящих событий.

   Ограничения при парсинге примеров событий

   При парсинге примеров данных, указанных в поле **Примеры событий**, в дополнительном нормализаторе не учитываются следующие параметры:

   - обогащение, настроенное в корневом нормализаторе;
   - фильтры, заданные в дополнительном нормализаторе;
   - значение параметра **Использовать сырое событие**;
   - преобразования в корневом нормализаторе;
   - преобразования для значения параметра **Поле, которое следует передать в нормализатор**.

9. В блоке параметров **Сопоставление** настройте сопоставление полей исходного события с полями событий Kaspersky SIEM Cloud:

   Таблица **Сопоставление** недоступна, если в поле **Метод парсинга** выбрано значение **normalizer**.

   a. Нажмите на кнопку **+ Добавить строку**.

      Вы можете добавить несколько строк таблицы или удалить строки таблицы. Для удаления строки таблицы установите рядом с ней флажок и нажмите на кнопку **Удалить**.

   b. В столбце **Исходные данные** укажите название поля исходного события, которое вы хотите сопоставить с полем события Kaspersky SIEM Cloud.

      Подробнее о формате названий полей см. в статье Модель данных нормализованного события. Описание сопоставления см. в статье Сопоставление полей предустановленных нормализаторов.

      Если вы хотите создать правила изменения полей исходного события перед записью в поля событий Kaspersky SIEM Cloud, нажмите на значок настройки (⚙) рядом с названием поля и в открывшемся окне **Преобразование** нажмите на кнопку **+ Добавить преобразование**. Вы можете изменить порядок правил и удалить правила. Для изменения порядка правил используйте значки изменения порядка (⠿). Для удаления правила нажмите рядом с ним на значок удаления (✕).

      Доступные преобразования

      Преобразования – это изменения, которые применяются к значению перед записью в поле события.

      Вы можете выбрать в раскрывающемся списке один из следующих типов преобразования:

      - **entropy** – используется для преобразования значения исходного поля с помощью функции вычисления информационной энтропии и помещения результата преобразования в целевое поле типа `float`. Результатом преобразования будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например, когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.
      - **lower** – используется для перевода всех символов значения в нижний регистр.

- **upper** – используется для перевода всех символов значения в верхний регистр.
- **regexp** – используется для преобразования значения с помощью указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.
- **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
  - **Символы на замену** – последовательность символов, которую требуется заменить.
  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.
- **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` требуется выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.
- **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.
- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.
- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.
  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.
- Конвертация закодированных строк в текст:
  - **decodeHexString** – используется для конвертации HEX-строки в текст.
  - **decodeBase64String** – используется для конвертации Base64-строки в текст.
  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.
  - **unicodeUnescape** – используется для конвертации Unicode-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, строка будет обрезана и не будет раскодирована.

Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.

Мы не рекомендуем использовать несколько дополнительных нормализаторов для последовательного преобразования одного и того же поля. Результат одного преобразования, выполненного дополнительным нормализатором, не используется как входные данные для следующего. В итоговое событие записывается значение, полученное в дополнительном нормализаторе, который первым выполнил обогащение этого поля.

- Преобразование формата IP-адреса в IPv4:
  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
- **hexToDecimal** – используется для преобразования числового значения, представленного в шестнадцатеричной системе счисления, в десятичный формат. Преобразование применяется к строковым или числовым полям, содержащим HEX-значения (включая префикс 0x, если он присутствует), и результат записывается в целевое поле события Kaspersky SIEM Cloud в виде целого числа.

  Результатом преобразования является число в десятичной системе, например исходное значение – 0x00FF, после преобразования – 255.

c. В столбце **Поле KUMA** в раскрывающемся списке выберите поле события Kaspersky SIEM Cloud. Вы можете найти поле события Kaspersky SIEM Cloud, введя его названия. Если название поля события Kaspersky SIEM Cloud начинается с `DeviceCustom*` и `Flex*`, при необходимости в поле **Подпись** укажите уникальную пользовательскую метку.

Если вы хотите, чтобы Kaspersky SIEM Cloud могла выполнить обогащение событий данными об активах и данные об активах были доступны в карточке алерта при срабатывании корреляционного правила, в таблице **Сопоставление** вам нужно настроить сопоставление полей для адреса хоста и имени хоста в зависимости от назначения актива. Например, вы можете настроить сопоставление для полей событий Kaspersky SIEM Cloud **SourceAddress** и **SourceHostName**, или **DestinationAddress** и **DestinationHostName**. В результате обогащения в карточке события появится поле события Kaspersky SIEM Cloud **SourceAssetID** или **DestinationAssetID** и ссылка, по которой можно будет перейти в карточку актива. В результате обогащения сведения об активе также будут доступны в карточке алерта.

Если вы загрузили данные в поле **Примеры событий**, в таблице отобразится столбец **Примеры** с примерами значений, переносимых из поля исходного события в поле события Kaspersky SIEM Cloud.

10. Если вы хотите добавлять дополнительные данные в созданные нормализованные события, создайте в нормализаторе правила обогащения, выполнив следующие действия:

a. Перейдите на вкладку **Обогащение**.

Вкладка **Обогащение** недоступна, если на вкладке **Схема нормализации** в поле **Метод парсинга** выбрано значение **normalizer**.

b. Нажмите на кнопку + **Добавить обогащение**.

Отобразится блок параметров правила обогащения. Вы можете добавить несколько правил обогащения или удалить правила обогащения. Для удаления правила обогащения нажмите рядом с ним на значок удаления (✕).

c. В раскрывающемся списке **Тип источника данных** выберите тип источника обогащения. При выборе определенных типов источника обогащения могут стать доступны дополнительные параметры, для которых вам нужно указать значения.

Доступные типы источников обогащения:

константа

Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "константа"

Параметр	Описание
Константа	Значение, которое требуется добавить в поле события. Максимальная длина значения – до 255 символов в кодировке Unicode. Если оставить поле пустым, существующее значение поля события будет удалено.
Целевое поле	Поле события, в которое требуется поместить данные.

Если вы используете функции обогащения событий для полей расширенной схемы с типом `Строка`, `Число` или `Число с плавающей точкой` с помощью константы, в поле будет добавлена константа.

Если вы используете функции обогащения событий для полей расширенной схемы с типом `Массив строк`, `Массив чисел` или `Массив чисел с плавающей точкой` с помощью константы, константа будет добавлена к элементам массива.

словарь

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "словарь"

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.

Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **словарь**, а в параметре **Ключевые поля обогащения** указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку в соответствии с правилами сериализации одного значения в формате TSV.

Пример. В параметре **Ключевые поля обогащения** используется поле расширенной схемы `SA.StringArrayOne`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`. В качестве ключа в словарь будут переданы значения `['a','b','c']`.

Если в параметре **Ключевые поля обогащения** используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом `|`.

Пример. В параметре **Ключевые поля обогащения** используется поле расширенной схемы `SA.StringArrayOne` и строковое поле `Code`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`, а строковое поле `Code` содержит последовательность символов `myCode`. В качестве ключа в словарь будут переданы значения `['a','b','c']|myCode`.

таблица

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "таблица"

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.
Сопоставление	Поля событий для передачи данных: • **Поле словаря** – поля словаря, из которых будут передаваться данные. Доступные поля зависят от выбранного ресурса словаря. • **Поле KUMA** – поля событий, в которые будут передаваться данные. Для выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** вы можете задать название для помещаемых данных.

Первое поле в таблице (**Поле словаря**) считается ключом, с которым будут сопоставляться поля, выбранные из события в качестве ключевых (**Поле KUMA**). В качестве ключа в **Поле словаря** вам нужно выбрать индикатор компрометации, по которому будет осуществляться обогащение, например IP-адрес, URL-адрес или хеш. В правиле необходимо выбрать поле события, соответствующее выбранному индикатору в поле словаря.

Если вы хотите выбрать несколько ключевых полей, вы можете указать их через разделитель `|` (при указании через веб-интерфейс или импорте через CSV-файл), например `<IP-адрес>|<имя пользователя>`.

Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить**. Для удаления строки таблицы нажмите на крестик ✕.

событие

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Доступные параметры типа обогащения описаны в таблице ниже.

Доступные параметры типа обогащения

Параметр	Описание
Целевое поле	Поле события Kaspersky SIEM Cloud, в которое требуется поместить данные.
Исходное поле	Поле события, значение которого будет записано в целевое поле.

Если вы хотите создать правило для изменения исходных данных перед записью в поля событий Kaspersky SIEM Cloud, в блоке параметров **Преобразование** нажмите на кнопку **+ Добавить преобразование**. В раскрывающемся списке **Тип** выберите нужный тип преобразования. Вы можете добавить несколько преобразований по кнопке **+ Добавить преобразование**. Чтобы удалить добавленное преобразование, нажмите рядом с ним на значок корзины.

Доступные преобразования

Преобразования – это изменения, которые применяются к значению перед записью в поле события.

Вы можете выбрать в раскрывающемся списке один из следующих типов преобразования:

- **entropy** – используется для преобразования значения исходного поля с помощью функции вычисления информационной энтропии и помещения результата преобразования в целевое поле типа `float`. Результатом преобразования будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например, когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.

- **lower** – используется для перевода всех символов значения в нижний регистр.

- **upper** – используется для перевода всех символов значения в верхний регистр.

- **regexp** – используется для преобразования значения с помощью указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.

- **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Символы на замену** – последовательность символов, которую требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

- **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` требуется выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.

- **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

- Конвертация закодированных строк в текст:

  - **decodeHexString** – используется для конвертации HEX-строки в текст.

  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  - **unicodeUnescape** – используется для конвертации Unicode-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.

Мы не рекомендуем использовать несколько дополнительных нормализаторов для последовательного преобразования одного и того же поля. Результат одного преобразования, выполненного дополнительным нормализатором, не используется как входные данные для следующего. В итоговое событие записывается значение, полученное в дополнительном нормализаторе, который первым выполнил обогащение этого поля.

- Преобразование формата IP-адреса в IPv4:
  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
- **hexToDecimal** – используется для преобразования числового значения, представленного в шестнадцатеричной системе счисления, в десятичный формат. Преобразование применяется к строковым или числовым полям, содержащим HEX-значения (включая префикс 0x, если он присутствует), и результат записывается в целевое поле события Kaspersky SIEM Cloud в виде целого числа.

  Результатом преобразования является число в десятичной системе, например исходное значение – 0x00FF, после преобразования – 255.

При использовании обогащения событий, у которых в качестве параметра **Тип источника данных** выбрано значение **событие**, а в качестве аргументов используются поля расширенной схемы событий, необходимо учесть следующие особенности:

- Если исходное поле расширенной схемы событий имеет тип `Массив строк`, а целевое поле расширенной схемы событий имеет тип `Строка`, значения будут размещены в целевом поле расширенной схемы событий в формате TSV.

  Пример: в поле расширенной схемы событий `SA.StringArray`, находятся значения `"string1"`, `"string2"`, `"string3"`. Выполняется операция обогащения событий. Результат выполнения операции обогащения событий заносится в поле расширенной схемы событий `DeviceCustomString1`. В поле расширенной схемы событий `DeviceCustomString1` будут находиться значения `["string1", "string2", "string3"]`.

- Если исходное и целевое поля расширенной схемы событий имеют тип `Массив строк`, значения целевого поля расширенной схемы событий будут дополнены значениями исходного поля расширенной схемы событий, а качестве символа-разделителя будет использован символ `","`.

  Пример: в поле расширенной схемы событий `SA.StringArrayOne`, находятся значения `["string1", "string2", "string3"]`, а в поле расширенной схемы событий `SA.StringArrayTwo` находятся значения `["string4", "string5", "string6"]`. Выполняется операция обогащения событий. Результат выполнения операции обогащения событий заносится в поле расширенной схемы событий `SA.StringArrayTwo`. В поле расширенной схемы событий `SA.StringArrayTwo` будут находиться значения `["string4", "string5", "string6", "string1", "string2", "string3"]`.

шаблон

Этот тип обогащения используется, если в поле события нужно записать значение, полученное при обработке шаблонов Go. Мы рекомендуем сопоставлять значение и размер поля. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "шаблон"

Параметр	Описание
Шаблон	Шаблон Go. Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт, например `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.
Целевое поле	Поле события, в которое требуется поместить данные.

Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **шаблон**, целевым полем является поле с типом `Строка`, а исходным полем является поле расширенной схемы событий, содержащее массив строк, то в шаблоне может быть использован один из следующих примеров:

- `{{.SA.StringArrayOne}}`
- ```
  {{- range $index, $element := . SA.StringArrayOne -}}
  {{- if $index}}, {{end}}"{{$element}}"{{- end -}}
  ```

Для преобразования в шаблоне данных поля массива в формат TSV требуется использовать функцию `toString`, например:

```
template {{toString .SA.StringArray}}
```

d. В раскрывающемся списке **Целевое поле** выберите поле события Kaspersky SIEM Cloud, в которое требуется поместить данные. Вы не можете выбрать значение, если в раскрывающемся списке **Исходный тип** вы выбрали **таблица**.

e. Если вы хотите включить детализацию в журнале нормализатора, включите переключатель **Отладка**. По умолчанию переключатель выключен.

f. Если вы хотите добавить несколько правил обогащения с разными типами источника данных, нажмите на кнопку + **Добавить обогащение** и настройте параметры.

Вы можете менять местами и удалять созданные правила. Для изменения места правила используйте значок ⣿ рядом с ним. Для удаления правила нажмите рядом с ним на значок ✕.

11. Нажмите кнопку **OK**.

12. Если вы хотите настроить дополнительный парсинг событий, выполните следующие действия:

a. Наведите курсор мыши на темный кружок и нажмите на отобразившийся значок плюса.

b. На вкладке **Условия дополнительной нормализации** настройте следующие параметры:

a. Если вы хотите передавать сырое событие для дополнительной нормализации, в раскрывающемся списке **Использовать сырое событие** выберите значение **Да**.

По умолчанию указано значение **Нет**. Мы рекомендуем передавать сырое событие в нормализаторы типа **json** и **xml**.

Также нужно выбрать значение **Да**, если вы хотите передавать сырое событие для дополнительной нормализации на второй, третий и далее уровень вложенности, последовательно на каждом уровне вложенности.

Параметр **Использовать сырое событие** не работает, если в основном правиле парсинга событий использован метод парсинга sql.
```

b. Если вы хотите отправлять на дополнительный парсинг только события с заданными в параметрах нормализатора полями, в поле **Поле, которое следует передать в нормализатор** укажите исходные поля события, которые должны быть переданы в дополнительный нормализатор.

Если оставить это поле пустым, в дополнительный нормализатор будет передано событие целиком.

Если при настройке параметров дополнительного нормализатора вы указали для параметра **Использовать сырое событие** значение **Нет** и значение в поле **Исходное поле** осталось незаполненным, любые настроенные преобразования для поля, которое передается в нормализатор, не будут работать. Чтобы преобразования выполнялись корректно, исходное поле должно быть заполнено либо указано значение **Да** для параметра **Использовать сырое событие**.

Kaspersky SIEM Cloud никак не ограничивает и не проверят текст, который вы указываете в этом параметре.

c. В блоке параметров **Параметры фильтров** настройте условия фильтрации, которым должны удовлетворять события, поступающие в нормализатор.

С помощью кнопки **Добавить условие** можно добавить строку с полями для определения условия (см. ниже). С помощью кнопки **Добавить группу** можно добавить группу фильтров. Можно переключать групповые операторы между **И**, **ИЛИ**, **НЕ**. В группы фильтров можно добавить другие группы условий и отдельные условия.

Условия и группы можно менять местами, перетягивая их за значок ⣿, а также удалять с помощью значка ✕.

Параметры условий фильтра:

- **Левый операнд** и **Правый операнд** – используются для указания значений, которые будет обрабатывать оператор.

  В левом операнде следует указывать исходное поле событий, поступающих в нормализатор. Например, если в окне **Основной парсинг событий** настроено сопоставление eventType - DeviceEventClass, то в окне **Дополнительный парсинг событий** на вкладке **Условия дополнительной нормализации** в поле левого операнда для фильтра следует указать eventType.

  Данные обрабатываются только как текстовые строки. Kaspersky SIEM Cloud никак не ограничивает и не проверят текст, который вы указываете в полях левого и правого операнда.

- Операторы:

  = – полное совпадение левого и правого операндов.

  startsWith – левый операнд начинается с символов, указанных в правом операнде.

  endsWith – левый операнд заканчивается символами, указанными в правом операнде.

  match – левый операнд соответствует регулярному выражению (RE2), указанному в правом операнде.

  in – левый операнд соответствует одному из значений, указанных в правом операнде.

Поступающие данные можно предварительно преобразовать, если нажать на кнопку 🔧: откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как над ними будут совершены какие-либо действия. В окне **Преобразования** добавленные правила можно менять местами, перетягивая их за значок ⣿, а также удалять с помощью значка ✕.

Доступные преобразования

Преобразования – это изменения, которые применяются к значению перед записью в поле события.

Вы можете выбрать в раскрывающемся списке один из следующих типов преобразования:

- **entropy** – используется для преобразования значения исходного поля с помощью функции вычисления информационной энтропии и помещения результата преобразования в целевое поле типа `float`. Результатом преобразования будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например, когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.

- **lower** – используется для перевода всех символов значения в нижний регистр.

- **upper** – используется для перевода всех символов значения в верхний регистр.

- **regexp** – используется для преобразования значения с помощью указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.

- **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.

- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Символы на замену** – последовательность символов, которую требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

- **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` требуется выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.

- **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

- Конвертация закодированных строк в текст:
  - **decodeHexString** – используется для конвертации HEX-строки в текст.
  - **decodeBase64String** – используется для конвертации Base64-строки в текст.
  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.
  - **unicodeUnescape** – используется для конвертации Unicode-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.

  Мы не рекомендуем использовать несколько дополнительных нормализаторов для последовательного преобразования одного и того же поля. Результат одного преобразования, выполненного дополнительным нормализатором, не используется как входные данные для следующего. В итоговое событие записывается значение, полученное в дополнительном нормализаторе, который первым выполнил обогащение этого поля.

- Преобразование формата IP-адреса в IPv4:
  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
- **hexToDecimal** – используется для преобразования числового значения, представленного в шестнадцатеричной системе счисления, в десятичный формат. Преобразование применяется к строковым или числовым полям, содержащим HEX-значения (включая префикс 0x, если он присутствует), и результат записывается в целевое поле события Kaspersky SIEM Cloud в виде целого числа.

  Результатом преобразования является число в десятичной системе, например исходное значение – 0x00FF, после преобразования – 255.

d. Перейдите на вкладку **Схема нормализации** и настройте параметры, как описано в шагах 2-9 инструкции.

e. Перейдите на вкладку **Обогащение** и настройте параметры, как описано в шаге 10 инструкции.

f. Нажмите кнопку **OK**.

13. Нажмите кнопку **Создать**.

В верхнем правом углу в поле поиска можно искать дополнительные правила парсинга по названию.

Для ресурсов нормализатора в полях ввода, кроме поля **Описание**, можно включить отображение непечатаемых символов.

Если вы, меняя параметры набора ресурсов коллектора, измените или удалите преобразования в подключенном к нему нормализаторе, правки не сохранятся, а сам нормализатор может быть поврежден. При необходимости изменить преобразования в нормализаторе, который уже является частью сервиса, вносите правки непосредственно в нормализатор в разделе веб-интерфейса **Ресурсы** → **Нормализаторы**.

Настройка дополнительной нормализации событий

В одном Syslog-источнике могут одновременно поступать события разных форматов, которые различаются по значению поля `PROCID` в заголовке Syslog.

В зависимости от значения `PROCID` содержимое поля `message` может иметь разную структуру.

Пример:

- `PROCID = application-A` – событие содержит сообщение в формате CEF.
- `PROCID = application-B` – событие содержит сообщение в формате JSON.

Так как структура поля `message` различается, необходимо настроить дополнительную нормализацию, которая позволит автоматически определять формат события и применять соответствующий метод парсинга.

Настройка дополнительной нормализации событий состоит из следующих этапов:

1. Создание основного нормализатора

Основной нормализатор принимает все входящие Syslog-события и выполняет базовую нормализацию полей.

Чтобы создать основной нормализатор:

1. В веб-интерфейсе перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Нормализаторы** и нажмите кнопку **Создать**.
2. В поле **Название** введите уникальное имя нормализатора. Максимальная длина имени: до 128 символов в кодировке Unicode.
3. В раскрывающемся списке **Тенант**, которому принадлежит нормализатор.
4. В раскрывающемся списке **Метод парсинга** выберите **syslog**.
5. В раскрывающемся списке **Сохранить исходное событие** выберите **Не сохранять**.
6. В блоке параметров **Сопоставление** нажмите на кнопку **Применить сопоставление по умолчанию**.
7. Нажмите на кнопку **OK**.

2 Создание экстранормализатора CEF

1. В окне с созданным нормализатором наведите курсор мыши на темный кружок и нажмите на отобразившийся значок плюса.
2. На вкладке **Условия дополнительной нормализации** в раскрывающемся списке **Использовать сырое событие** выберите **Нет**.
3. В блоке параметров **Параметры фильтра** нажмите на кнопку **Добавить условие** и настройте параметры фильтрации:
   a. В левом операнде введите:

   ```
   PROCID
   ```

   b. В качестве оператора выберите **=**.
   c. В правом операнде введите:

   ```
   application-A
   ```

4. Перейдите на вкладку **Схема нормализации**.
5. В поле **Название** введите:

   ```
   cef
   ```

6. В раскрывающемся списке **Метод парсинга** выберите **cef**.
7. В блоке параметров **Сопоставление** нажмите на кнопку **Применить сопоставление по умолчанию**.
8. Нажмите на кнопку **OK**.

События с `PROCID = application-A` направляются в CEF-парсер и нормализуются в модель Kaspersky SIEM Cloud.

3 Создание экстранормализатора JSON

1. В окне с созданным нормализатором наведите курсор мыши на темный кружок и нажмите на отобразившийся значок плюса.
2. На вкладке **Условия дополнительной нормализации** в раскрывающемся списке **Использовать сырое событие** выберите **Нет**.
3. В блоке параметров **Параметры фильтра** нажмите на кнопку **Добавить условие** и настройте параметры фильтрации:
   a. В левом операнде введите:

   ```
   PROCID
   ```

b. В качестве оператора выберите **=**.

c. В правом операнде введите:

```
application-B
```

4. Перейдите на вкладку **Схема нормализации**.

5. В поле **Название** введите:

```
json
```

6. В раскрывающемся списке **Метод парсинга** выберите **json**.

7. В блоке параметров **Сопоставление** нажмите на кнопку **Применить сопоставление по умолчанию**.

8. Нажмите на кнопку **OK**.

События с `PROCID = application-B` направляются в JSON-парсер и нормализуются в модель Kaspersky SIEM Cloud.

4 Проверка работы дополнительной нормализации

После настройки экстранормализаторов рекомендуется проверить, правильно ли вы настроили маршрутизацию и обработку событий.

Проверьте следующее:

- События с `PROCID = application-A` передаются в экстранормализатор **CEF**.
- События с `PROCID = application-B` передаются в экстранормализатор **JSON**.
- После обработки оба типа событий приводятся к модели данных Kaspersky SIEM Cloud.

Для проверки отправьте в Kaspersky SIEM Cloud тестовые события, соответствующие каждому из настроенных условий, и убедитесь, что они успешно нормализуются.

Ожидаемый результат:

- CEF-события обрабатываются парсером **cef**.
- JSON-события обрабатываются парсером **json**.
- Нормализованные события отображаются в разделе **События** и содержат поля, сопоставленные со схемой Kaspersky SIEM Cloud.

Переиспользование нормализаторов

Некоторые предустановленные нормализаторы Kaspersky SIEM Cloud, например **[OOTB] Apache Access file**, **[OOTB] Nginx regexp**, **[OOTB] BIND file** и **[OOTB] Squid access.log file**, предназначены для обработки событий, поступающих из файлов журналов. Если те же события поступают по протоколу Syslog, сообщение дополнительно содержит заголовок Syslog, который необходимо обработать перед разбором содержимого сообщения.

Чтобы не создавать отдельные нормализаторы для каждого варианта получения событий, можно настроить каскадную нормализацию. В этом случае сначала выполняется обработка заголовка с помощью предустановленного нормализатора **[OOTB] Syslog header**, после чего событие передается соответствующему OOTB-нормализатору для разбора содержимого сообщения. Таким образом можно использовать один и тот же нормализатор независимо от способа получения событий.

Чтобы настроить каскадную нормализацию:

1. В веб-интерфейсе Kaspersky SIEM Cloud откройте раздел **Мониторинг → Ресурсы и сервисы → Коллекторы**.
2. В списке доступных коллекторов найдите и выберите предустановленный коллектор **[OOTB] Apache Access file**.
3. В открывшемся окне перейдите в раздел **Парсинг событий** и на вкладке **Схемы парсинга** нажмите на кнопку **Добавить парсинг событий**.
4. На вкладке **Схема нормализации** в раскрывающемся списке **Нормализатор** выберите **[OOTB] Syslog header**.
5. Нажмите на кнопку **OK**.
6. В окне с добавленным нормализатором наведите курсор мыши на темный кружок и нажмите на отобразившийся значок плюса, чтобы добавить экстранормализатор.
7. В открывшемся окне перейдите на вкладку **Схема нормализации**.
8. В раскрывающемся списке **Метод парсинга** выберите **normalizer**.
9. В раскрывающемся списке **Нормализатор** выберите **[OOTB] Apache Access file**.
10. Нажмите на кнопку **OK**.
11. Сохраните настроенные параметры коллектора.
12. Повторите шаги 2–11, чтобы настроить коллекторы **[OOTB] Nginx regexp**, **[OOTB] BIND file** и **[OOTB] Squid access.log file**, добавляя в качестве экстранормализатора соответствующий OOTB-нормализатор.

После настройки убедитесь, что события, поступающие по протоколу Syslog, последовательно проходят оба этапа нормализации:

- Нормализатор **[OOTB] Syslog header** извлекает поля заголовка Syslog.
- OOTB-нормализатор соответствующего типа журнала выполняет разбор содержимого сообщения и приводит событие к модели данных Kaspersky SIEM Cloud.

Результат обработки можно проверить в веб-интерфейсе Kaspersky SIEM Cloud в разделе **События**.

Использование расширенной схемы событий для нормализации

От источников могут приходить события с данными, которые не укладываются в набор полей формата событий CEF. Шести уже имеющихся дополнительных полей `DeviceCustomString`, предусмотренных форматом CEF, может быть недостаточно для сопоставления таких данных. Поэтому в Kaspersky SIEM Cloud есть возможность создать дополнительные поля, которые называются *полями расширенной схемы событий*. С полями расширенной схемы событий вы можете сопоставить поля полученного события. Такая настройка позволит вам сохранять полученные нестандартные данные в нормализованном событии.

Вы можете использовать поля расширенной схемы событий в нормализаторах для нормализации событий и в других ресурсах Kaspersky SIEM Cloud, например, в качестве полей виджетов, а также в SQL-запросах для фильтрации и поиска событий, в таблице событий и пресетах.

Список всех полей расширенной схемы событий, существующих в Kaspersky SIEM Cloud, доступен в разделе **Поля расширенной схемы событий**.

Рекомендации и ограничения

Использование значительного количества уникальных полей расширенной схемы событий может привести к снижению производительности системы, увеличению объема дискового пространства, необходимого для хранения событий и сложности восприятия данных.

С точки зрения нагрузки на сервер хранения при операциях поиска событий, подготовки отчетов и других операций с событиями в хранилище наиболее предпочтительными являются поля схемы событий KUMA, после чего идут поля расширенной схемы событий, затем поля `Extra`.

При использовании полей расширенной схемы событий сохраняется общее ограничение для максимального размера события обрабатываемого коллектором – 4 МБ.

Типизация

Поля расширенной схемы событий имеют строгую типизацию, приведенную в таблице ниже.

Тип	Доступность в нормализаторе	Тип данных
`S`	Все типы	Строка.
`N`	Все типы	Число.
`F`	Все типы	Число с плавающей точкой.
`SA`	KV, JSON	Массив строк. Порядок элементов массива соответствует порядку элементов сырого события.
`NA`	KV, JSON	Массив целых чисел. Порядок элементов массива соответствует порядку элементов сырого события.
`FA`	KV, JSON	Массив чисел с плавающей точкой. Порядок элементов массива соответствует порядку элементов сырого события.

Если данные, находящиеся в полях сырого события, не соответствуют типу поля Kaspersky SIEM Cloud, в процессе нормализации событий значение не будет сохранено, если невозможно выполнить преобразование типов данных. Например, строка `test` не может быть помещена в числовое поле KUMA `DeviceCustomNumber1`.

Служебные и пользовательские поля расширенной схемы событий

В расширенной схеме событий помимо пользовательских полей, которые вы можете добавлять сами, в Kaspersky SIEM Cloud зарезервированы служебные поля. В служебные поля вы не можете нормализовывать пользовательские данные. Вы не можете изменять, удалять, экспортировать и отключать служебные поля. Все поля расширенной схемы событий с префиксом `KL_` являются служебными и управляются только с серверов "Лаборатории Касперского". Мы не рекомендуем использовать префикс `KL_` в имени при добавлении новых полей расширенной схемы событий.

По умолчанию в Kaspersky SIEM Cloud автоматически добавляются следующие служебные поля расширенной схемы событий:

- `KL_EventRoute`, тип `S` – предназначено для хранения информации о маршруте события.

  Вы можете использовать это поле в нормализаторах, в качестве ключа или значения в активных листах, в правилах обогащения, в качестве поля запроса в правилах сбора и анализа данных, в корреляционных правилах. Вы не можете использовать это поле для детектирования источников событий.

- `KL_AI_DLLHijackingCheckResult`, тип `N` – предназначено для хранения информации о результате проверки динамической библиотеки, которая потенциально может использоваться в атаках типа DLL Hijacking. Результат проверки выдает сервис KSN.

- Следующие поля добавлены в корреляционное событие:

  - `KL_CorrelationRulePriority`, тип `N`;
  - `KL_SourceAssetDisplayName`, тип `S`;
  - `KL_DestinationAssetDisplayName`, тип `S`;
  - `KL_DeviceAssetDisplayName`, тип `S`;
  - `KL_SourceAccountDisplayName`, тип `S`;
  - `KL_DestinationAccountDisplayName`, тип `S`.

  Вы можете использовать эти служебные поля для поиска событий.

Использование полей расширенной схемы событий

Настройка нормализации данных в поле расширенной схемы событий состоит из следующих этапов:

1. **Добавление нового поля расширенной схемы событий**

   Если поле полученного события не может быть нормализовано в одно из полей формата событий CEF, включая шесть дополнительных полей DeviceCustomString, добавьте новое поле расширенной схемы событий.

2. **Сопоставление полей в нормализаторе**

   Сопоставьте поле сырого события и новое поле расширенной схемы событий:

   1. Откройте существующий или создайте новый нормализатор.
   2. Заполните основные параметры нормализатора.
   3. В блоке параметров **Сопоставление** нажмите на кнопку **Добавить строку**.

4. В параметре **Исходные данные** укажите название исходного поля в сыром событии.

5. В параметре **Поле KUMA** начните вводить имя поля расширенной схемы событий и выберите нужное поле в раскрывающемся списке.

   Поля расширенной схемы событий в раскрывающемся списке имеют имя в формате `<тип>.<имя поля>`.

6. Нажмите на кнопку **Сохранить** для сохранения нормализатора событий.

Поле сырого события нормализуется в выбранное поле расширенной схемы событий.

Просмотр таблицы полей расширенной схемы событий

Список всех полей расширенной схемы событий, существующих в Kaspersky SIEM Cloud, доступен в разделе **Параметры → KUMA → Открыть параметры KUMA → Поля расширенной схемы событий**. Список полей расширенной схемы событий единый для всех тенантов.

Просматривать таблицу полей расширенной схемы событий могут только пользователи с ролями Главный администратор, Администратор тенанта, Аналитик второго уровня, Аналитик первого уровня, Младший аналитик, Чтение общих ресурсов, Редактирование общих ресурсов.

Таблица **Поля расширенной схемы событий** содержит следующие данные:

- **Тип** – тип данных поля расширенной схемы событий.

  Доступные типы данных

Тип	Доступность в нормализаторе	Тип данных
S	Все типы	Строка.
N	Все типы	Число.
F	Все типы	Число с плавающей точкой.
SA	KV, JSON	Массив строк. Порядок элементов массива соответствует порядку элементов сырого события.
NA	KV, JSON	Массив целых чисел. Порядок элементов массива соответствует порядку элементов сырого события.
FA	KV, JSON	Массив чисел с плавающей точкой. Порядок элементов массива соответствует порядку элементов сырого события.

- **Имя поля** – имя поля расширенной схемы событий, без типа.

  Вы можете нажать на имя, чтобы изменить параметры поля расширенной схемы событий.

- **Статус** – возможность использовать поле расширенной схемы событий в ресурсах.

  Вы можете перевести переключатель в положение **Включено** или **Выключено**, чтобы разрешить или запретить использование этого поля расширенной схемы событий в новых ресурсах. При этом выключенное поле все еще будет использоваться в уже работающих конфигурациях ресурсов, пока вы не удалите его из конфигурации вручную, а также будет доступно в списке столбцов таблицы в разделе **События** для работы со старыми событиями.

  Выключить использование поля расширенной схемы событий может только пользователь с ролью Главный администратор.

- **Дата обновления** – дата и время последнего изменения поля расширенной схемы событий.

- **Создал** – имя пользователя, который создал поле расширенной схемы событий.

- **Зависимости** – количество ресурсов Kaspersky SIEM Cloud, макетов панели мониторинга, отчетов, пресетов и наборов полей для поиска источников событий, использующих поле расширенной схемы событий.

  Вы можете нажать на число, чтобы открыть панель с таблицей всех ресурсов и других сущностей Kaspersky SIEM Cloud, в которых используется это поле. Для каждой зависимости в таблице отображается название, тенант (только для ресурсов) и тип. Зависимости в таблице отсортированы по названию. Вы можете нажать на название зависимости, чтобы перейти на ее страницу (кроме макетов панели мониторинга, пресетов и сохраненных запросов пользователей).

  Вы можете просмотреть зависимости поля расширенной схемы событий только от тех ресурсов и сущностей, к тенантам которых у вас есть доступ. Если у вас нет доступа к тенанту, соответствующие ресурсы не будут отображаться в таблице, но будут учитываться в количестве зависимостей.

- **Описание** – текстовое описание поля.

По умолчанию таблица полей расширенной схемы событий отсортирована по убыванию даты обновления. При необходимости вы можете отсортировать таблицу, нажав на заголовок столбца и выбрав **По возрастанию** или **По убыванию**, а также воспользоваться контекстным поиском по имени поля.

Добавление, изменение и удаление полей расширенной схемы событий

Пользователи с ролями Главный администратор, Администратор тенанта, Аналитик второго уровня, Аналитик первого уровня, Младший аналитик, Редактирование общих ресурсов могут добавлять новые и изменять существующие поля расширенной схемы событий. Удалять поля могут только пользователи с ролью Главный администратор.

Добавление полей

Чтобы добавить поле расширенной схемы событий:

1. В веб-интерфейсе перейдите в раздел **Параметры → KUMA → Открыть параметры KUMA → Поля расширенной схемы событий** и нажмите на кнопку **Добавить**.

2. Включите или выключите переключатель **Статус**, чтобы разрешить или запретить использовать это поле расширенной схемы событий в ресурсах.

   По умолчанию переключатель включен. Выключенное поле все еще будет доступно в списке столбцов таблицы в разделе **События** для работы со старыми событиями.

3. В поле **Тип** выберите тип данных поля расширенной схемы событий.

   Доступные типы данных

Тип	Доступность в нормализаторе	Тип данных
S	Все типы	Строка.
N	Все типы	Число.
F	Все типы	Число с плавающей точкой.
SA	KV, JSON	Массив строк. Порядок элементов массива соответствует порядку элементов сырого события.
NA	KV, JSON	Массив целых чисел. Порядок элементов массива соответствует порядку элементов сырого события.
FA	KV, JSON	Массив чисел с плавающей точкой. Порядок элементов массива соответствует порядку элементов сырого события.

4. В поле **Имя поля** укажите имя поля расширенной схемы событий.

Имя поля расширенной схемы событий имеет следующие особенности:

- Должно быть уникальным в рамках инсталляции Kaspersky SIEM Cloud.
- Чувствительно к регистру. Например, имена `Имя_поля` и `имя_поля` считаются разными именами.
- Допустимо использовать символы латиницы, кириллицы и числа. Не допускается использование пробелов и символов " ~ ` @ # $ % ^ & * ( ) + - [ ] { } | \ | / . " < > ; ! , : ? =.
- Если вы хотите использовать поля расширенной схемы событий для поиска источников событий, допустимо использовать только символы латиницы и числа.
- Максимальная длина – 128 символов.

5. При необходимости в поле **Описание** укажите описание поля расширенной схемы событий.

   Мы рекомендуем в описании указывать назначение добавляемого поля расширенной схемы событий. В описании допустимо использовать только символы Unicode. Максимальная длина – 256 символов.

6. Нажмите на кнопку **Сохранить**.

Новое поле расширенной схемы событий будет добавлено и отобразится в начале таблицы. Будет создано событие аудита о создании поля расширенной схемы событий. Если вы включили поле, вы сможете использовать его в нормализаторах и при конфигурации ресурсов.

Изменение полей

Чтобы изменить поле расширенной схемы событий:

1. В веб-интерфейсе в разделе **Параметры → KUMA → Открыть параметры KUMA → Поля расширенной схемы событий** нажмите на название поля, которое вы хотите изменить.

   Откроется панель **Редактирование расширенной схемы**. В этой панели отображаются параметры выбранного поля, а также таблица **Зависимости** со списком ресурсов, макетов панели мониторинга, отчетов, пресетов и наборов полей для поиска источников событий, в которых используется это поле. Отображаются только те ресурсы, к тенантам которых у вас есть доступ. Если поле используется в тех ресурсах, к тенантам которых у вас нет доступа, эти ресурсы не будут отображаться в таблице.

   Вы можете нажать на название ресурса или сущности, чтобы перейти на его страницу (кроме ресурсов панели мониторинга, пресетов и сохраненных запросов пользователей).

2. Внесите необходимые изменения в доступные параметры.

   Вы можете изменить параметры **Тип** и **Имя поля**, только если у этого поля расширенной схемы событий нет зависимостей. Параметры **Статус** и **Описание** вы можете изменить для любого поля расширенной схемы событий. Поле со статусом **Выключено** все еще будет использоваться в уже работающих конфигурациях ресурсов, пока вы не удалите его из конфигурации вручную, а также будет доступно в списке столбцов таблицы в разделе **События** для работы со старыми событиями.

   Выключить использование поля расширенной схемы событий с помощью переключателя **Статус** может только пользователь с ролью Главный администратор.

3. Нажмите на кнопку **Сохранить**.

Поле расширенной схемы событий обновлено. Будет создано событие аудита об изменении поля.

Удаление полей

Вы можете удалить только те поля расширенной схемы событий, которые не являются служебными, у которых установлен статус **Выключено** и которые не используются в ресурсах и других сущностях Kaspersky SIEM Cloud (нет зависимостей). Мы рекомендуем удалять поля расширенной схемы событий через некоторые время после того, как события, в которых использовалось поле, были гарантированно удалены из Kaspersky SIEM Cloud. После удаления поле не будет отображаться в подсказках событий.

Чтобы удалить поля расширенной схемы событий:

1. В веб-интерфейсе перейдите в раздел **Параметры → KUMA → Открыть параметры KUMA → Поля расширенной схемы событий**

2. Установите флажки в первом столбце таблицы напротив одного или нескольких полей, которые вы хотите удалить.

   Вы можете выбрать все поля, установив флажок в первом столбце заголовка таблицы.

3. Нажмите на кнопку **Удалить** в верхней части таблицы.

   Кнопка **Удалить** активна, только если все выбранные поля выключены и не имеют зависимостей. Если хотя бы одно поле включено или имеет зависимость, кнопка неактивна.

   Если вы хотите удалить поле, которое используется хотя бы в одном ресурсе Kaspersky SIEM Cloud, но у вас нет доступа к его тенанту, кнопка **Удалить** будет активна при выборе этого поля, но при попытке удалить его отобразится ошибка.

Выбранные поля будут удалены. Будет создано событие аудита об удалении полей.

Импорт и экспорт полей расширенной схемы событий

Вы можете добавить сразу несколько новых полей расширенной схемы событий, импортировав их из файла в формате JSON. Вы также можете экспортировать все существующие в Kaspersky SIEM Cloud поля расширенной схемы событий с информацией о них в файл, например, для передачи списка полей в другие инсталляции Kaspersky SIEM Cloud для поддержания работы ресурсов.

Импортировать и экспортировать поля расширенной схемы событий могут пользователи с ролями Главный администратор, Администратор тенанта, Аналитик второго уровня, Аналитик первого уровня, Младший аналитик, Редактирование общих ресурсов. Пользователи с ролью Чтение общих ресурсов могут только экспортировать поля расширенной схемы событий.

Чтобы импортировать поля расширенной схемы событий в Kaspersky SIEM Cloud из файла:

1. В веб-интерфейсе перейдите в раздел **Параметры → KUMA → Открыть параметры KUMA → Поля расширенной схемы событий** и нажмите на кнопку **Импортировать**.

2. В открывшемся окне выберите файл в формате JSON со списком объектов полей расширенной схемы событий.

Пример файла JSON

```
[
{"kind": "SA",
"name": "<fieldName1>",
"description": "<description1>",
"disabled": false},
{"kind": "N",
"name": "<fieldName2>",
"description": "<description2>",
"disabled": false},
....
{"kind": "FA",
"name": "<fieldNameX>",
"description": "<descriptionX>",
"disabled": false}
]
```

При импорте полей из файла их имена проверяются на возможные конфликты внутри одного типа. Если в Kaspersky SIEM Cloud уже существует поле с таким названием и типом, такие поля из файла не будут импортированы.

Поля расширенной схемы событий будут импортированы из файла в Kaspersky SIEM Cloud. Будет создано событие аудита об импорте полей, а также на каждое добавляемое поле будет создано отдельное событие аудита.

Чтобы экспортировать поля расширенной схемы событий в файл:

1. В веб-интерфейсе перейдите в раздел **Параметры → KUMA → Открыть параметры KUMA → Поля расширенной схемы событий**.

2. Выполните одно из следующих действий:

   - Если вы хотите экспортировать конкретные поля расширенной схемы событий, выполните следующие действия:

     a. Установите флажки в первом столбце таблицы напротив необходимых полей. Вы не можете выбрать служебные поля.

     b. Нажмите на кнопку **Экспортировать выбранные** в верхней части таблицы.

   - Если вы хотите экспортировать все поля расширенной схемы событий, нажмите на кнопку **Экспортировать все** в верхней части таблицы.

Файл JSON со списком объектов полей расширенной схемы событий и информацией о них будет скачан.

Использование коннектора

Коннекторы используются для установления соединений между сервисами Kaspersky SIEM, а также для активного и пассивного получения событий.

Некоторые типы коннекторов (например, tcp, sql, wmi, wec и etw) поддерживают шифрование с использованием протокола TLS. Решение поддерживает протокол TLS версии 1.2 или 1.3. При включении режима TLS для этих коннекторов подключение осуществляется по следующему алгоритму:

- Если Kaspersky SIEM используется в качестве клиента:

  1. Решение отправляет запрос на соединение с сервером с максимальной поддерживаемой версией протокола TLS 1.3 ClientHello, а также список поддерживаемых криптонаборов.

  2. Сервер отвечает на запрос выбранной версией протокола TLS и криптонабора.

  3. В зависимости от версии протокола TLS в ответе сервера:

     - Если сервер отвечает на запрос, используя TLS 1.3 или 1.2, Kaspersky SIEM Cloud установит соединение с сервером.

     - Если сервер отвечает на запрос, используя TLS 1.1, Kaspersky SIEM Cloud закроет соединение с сервером.

- Если решение используется в качестве сервера:

  1. Клиент отправляет запрос на соединение с Kaspersky SIEM Cloud с максимальной поддерживаемой версией протокола TLS, а также список поддерживаемых криптонаборов.

  2. В зависимости от версии протокола TLS в запросе клиента:

     - Если в запросе клиента используется протокол TLS 1.1 ClientHello, Kaspersky SIEM Cloud закроет соединение.

     - Если в запросе клиента используется протокол TLS 1.2 или 1.3, Kaspersky SIEM Cloud ответит на запрос выбранной версией протокола TLS и криптонабора.

Чтобы создать коннектор:

1. В веб-интерфейсе решения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Коннекторы** и нажмите кнопку **Создать**.

2. В раскрывающемся списке **Тип** выберите тип коннектора и укажите его параметры на вкладках **Основные параметры** и **Дополнительные параметры**:

   - internal
   - tcp
   - udp
   - netflow

- sflow
- nats-jetstream
- kafka
- http
- sql
- file
- 1c-log
- 1c-xml
- diode
- ftp
- sftp
- nfs
- wmi
- wec
- etw
- snmp
- snmp-trap
- kata/edr
- vmware
- elastic
- office365
- dfi
- universalAPI
- smb
- http-streaming

3. Нажмите кнопку **Создать**.

Параметры коннекторов

Этот раздел содержит описание параметров всех поддерживаемых Kaspersky SIEM Cloud типов коннекторов.

Вы можете просмотреть параметры созданных коннекторов в разделе **Мониторинг** → **Ресурсы и сервисы** → **Коннекторы**, выбрав нужный коннектор из списка.

Коннектор, тип internal

Коннекторы с типом **internal** в основном используются для приема событий от агента в коллектор по протоколу internal.

Коннектор с этим типом также используется для приема следующих данных:

- Внутренние данные, такие как маршруты событий.
- Файловые атрибуты. Если при создании коллектора на шаге Транспорт мастера установки вы указали коннектор с типом file, на шаге **Парсинг событий** в таблице **Сопоставление** вы можете передать в поле события Kaspersky SIEM Cloud название обрабатываемого коллектором файла или путь к файлу. Для этого в столбце **Исходные данные** укажите одно из следующих значений:
  - `$kuma_fileSourceName` – передать в поле события Kaspersky SIEM Cloud название обрабатываемого коллектором файла.
  - `$kuma_fileSourcePath` – передать в поле события Kaspersky SIEM Cloud путь к обрабатываемому коллектором файлу.

  Когда вы используете коннектор с типом **file**, новые переменные в нормализаторе будут работать только с точками назначения с типом internal.
- События в маршрутизатор событий. Маршрутизатор событий может принимать события только по протоколу internal, поэтому при отправке событий в маршрутизатор событий вы можете использовать только точки назначения с типом **internal**.

Доступные параметры коннектора с типом **internal** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **internal**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.

Параметр	Описание
URL	URL-адрес и номер порта, который прослушивает коннектор. Вы можете ввести значение в одном из следующих форматов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `:<port number>`. IPv6-адреса можно указать в формате `[<IPv6 address>%<interface>:<port number>`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Можно добавить только один URL-адрес. Если значение поля содержит пробелы или символы табуляции, невозможно сохранить ресурс или сервис. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.

Коннектор, тип tcp

Коннекторы с типом **tcp** используются для пассивного получения событий по протоколу TCP при работе с агентами Windows и Linux. Доступные параметры коннектора с типом **tcp** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **tcp**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Вы можете ввести URL-адрес в одном из следующих форматов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address>:<port number>`; • `:<port number>`. Обязательный параметр.

Параметр	Описание
Auditd	Переключатель, включающий механизм auditd, который группирует полученные от коннектора строки событий auditd в одно с auditd. Если вы включили этот переключатель, вы не можете выбрать значение в раскрывающемся списке **Разделитель**, так как для м auditd автоматически выбирается значение **\n**. Если вы включили этот переключатель в параметрах коннектора агента, вам нужно выбрать значение **\n** в раскрывающемся с **Разделитель** в параметрах коннектора коллектора, в который агент отправляет события. Максимальный размер сгруппированного события auditd составляет примерно 4 174 304 символов. Kaspersky SIEM Cloud классифицирует события Auditd в соответствии с алгоритмом. Например, для обработки получены сл записи: `type=LOGIN msg=audit(1712820601.957:21458): pid=4987 uid=0 subj=0:63:0:0 old-auid=4294967295 auid=0 tty old-ses=4294967295 ses=2348 res=1` `type=SYSCALL msg=audit(1712820601.957:21458): arch=c000003e syscall=1 success=yes exit=1 a0=7 a1=7ffc9a a3=0 items=0 ppid=429 pid=4987 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none comm="cron" exe="/usr/sbin/cron" subj=0:63:0:0 key=(null)` `type=PROCTITLE msg=audit(1712820601.957:21458): proctitle=2F7573722F7362696E2F43524F4E002D66` В соответствии с алгоритмом в этом случае мы получим одно однострочное событие с типом LOGIN, так как тип LOGIN имеет он меньше AUDIT_FIRST_EVENT равного 1300, и одно многострочное событие с SYSCALL и PROCTITLE. При группировке многострочного события auditd, содержащего записи с разными префиксами, в итоговом событии будет исп префикс той записи, которая пришла первой. Это необходимо для корректного парсинга события нормализатором. Например обработки получены следующие записи: `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE msg=audit(1742441361.524:787467): proctitle=686170726F7879002D57002D6462002D66002F7573722F6C6F63616C2F6574632F686170726F78792F686170726F7` `<182>2025-03-20T06:29:22.643145+03:00 test-server-01 tag_audit_log: type=SOCKADDR msg=audit(1742441361.524:787467): saddr=020026FC0A5E41E80000000000000000` `<182>2025-03-20T06:29:22.643143+03:00 test-server-01 tag_audit_log: type=SYSCALL msg=audit(1742441361.5 arch=c000003e syscall=42 success=no exit=-115 a0=1b a1=55d3f02e8c80 a2=10 a3=55d3eec440d0 items=0 ppid= pid=1356 auid=4294967295 uid=99 gid=99 euid=99 suid=99 fsuid=99 egid=99 sgid=99 fsgid=99 tty=(none) ses comm="haproxy" exe="/usr/local/sbin/haproxy" subj=docker-default key="network_events"<` Поскольку первой пришла запись `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE msg=audit(...)`, то в итоговом событии будет использоваться префикс `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log:`. При группировке событий решение игнорирует строки с типом `EOE` (например, `type=EOE msg=audit(1633859647.072:1206`) поскольку они не передают важной для событий информации.
Разделитель	• **\n** (используется по умолчанию); • **\t**; • **\0**.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Параметр	Описание
TTL буфера событий	Время жизни буфера для строк событий auditd в миллисекундах. Строки событий auditd попадают в коллектор Kaspersky SIEM Cloud и накапливаются в буфере. Это позволяет сгруппировать несколько строк событий auditd в одно событие auditd. Отсчет времени жизни буфера начинается при получении первой строки события auditd или при истечении предыдущего времени жизни буфера. Доступные значения: от 50 до 30 000. Значение по умолчанию: `2000`. Это поле доступно, если вы включили переключатель **Auditd** на вкладке **Основные параметры**. Строки событий auditd, накопленные в буфере, хранятся в оперативной памяти сервера. Мы рекомендуем с осторожностью увеличивать размер буфера, так как это может привести к использованию слишком большого количества оперативной памяти сервера коллектором Kaspersky SIEM Cloud. Вы можете просмотреть в метриках Kaspersky SIEM Cloud, сколько оперативной памяти сервера использует коллектор Kaspersky SIEM Cloud. Если вы хотите, чтобы время жизни буфера составляло более 30 000 миллисекунд, мы рекомендуем использовать другой транспорт доставки событий auditd. Например, вы можете использовать агента или предварительно накапливать события auditd в файле, после чего обрабатывать файл коллектором Kaspersky SIEM Cloud.
Заголовок транспорта	Регулярное выражение для событий auditd, по которому определяются строки событий auditd. Вы можете использовать значение по умолчанию или изменить его. Регулярное выражение должно содержать группы `record_type_name`, `record_type_value` и `event_sequence_number`. Если многострочное событие auditd содержит префикс, для первой строки события auditd префикс сохраняется, а для последующих – отбрасывается. Вы можете вернуться регулярному выражению для событий auditd по умолчанию, нажав на кнопку **Установить значение по умолчанию**.

Параметр	Описание
Режим TLS	Режим шифрования TLS. При использовании шифрования TLS вы не можете указать IP-адрес в поле URL на вкладке **Основные параметры**. Доступные значения: • **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию. • **Включено** – использовать шифрование TLS, но без верификации сертификатов. • **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс Kaspersky SIEM Cloud в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать PFX-секрет?** *Чтобы создать PFX-секрет:* 1. В поле **Название** введите название PFX-секрета. 2. Нажмите на кнопку **Загрузить PFX** и выберите файл в формате PKCS#12-контейнера, в который вы экспортировали файл PFX с закрытым ключом. 3. В поле **Пароль** введите пароль для защиты файла PFX, указанный в мастере экспорта PFX. 4. Нажмите на кнопку **Создать**. PFX-секрет будет создан и отобразится в раскрывающемся списке **PFX секрет**. • **Нестандартный PFX с аутентификацией клиента** – использовать шифрование TLS с PFX-секретом. В этом режиме выполняется аутентификация клиента по сертификату. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс Kaspersky SIEM Cloud в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать PFX-секрет?** *Чтобы создать PFX-секрет:* 1. В поле **Название** введите название PFX-секрета. 2. Нажмите на кнопку **Загрузить PFX** и выберите файл в формате PKCS#12-контейнера, в который вы экспортировали файл PFX с закрытым ключом. 3. В поле **Пароль** введите пароль для защиты файла PFX, указанный в мастере экспорта PFX. 4. Нажмите на кнопку **Создать**. PFX-секрет будет создан и отобразится в раскрывающемся списке **PFX секрет**.
Сжатие	Определяет метод распаковки данных, поступающих в коннектор. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.

Коннектор, тип udp

Коннекторы с типом **upd** используются для пассивного получения событий по протоколу UDP при работе с агентами Windows и Linux. Доступные параметры коннектора с типом **udp** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.

Параметр	Описание
Тип	Тип коннектора – **udp**. Обязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Вы можете ввести URL-адрес в одном из следующих форматов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address>:<port number>`; • `:<port number>`. Обязательный параметр.
Auditd	Переключатель, включающий механизм auditd, который группирует полученные от коннектора строки событий auditd в одно с auditd. Если вы включили этот переключатель, вы не можете выбрать значение в раскрывающемся списке **Разделитель**, так как для м auditd автоматически выбирается значение **\n**. Если вы включили этот переключатель в параметрах коннектора агента, вам нужно выбрать значение **\n** в раскрывающемся с **Разделитель** в параметрах коннектора коллектора, в который агент отправляет события. Максимальный размер сгруппированного события auditd составляет примерно 4 174 304 символов. Kaspersky SIEM Cloud классифицирует события Auditd в соответствии с алгоритмом. Например, для обработки получены сл записи: `type=LOGIN msg=audit(1712820601.957:21458): pid=4987 uid=0 subj=0:63:0:0 old-auid=4294967295 auid=0 tty old-ses=4294967295 ses=2348 res=1` `type=SYSCALL msg=audit(1712820601.957:21458): arch=c000003e syscall=1 success=yes exit=1 a0=7 a1=7ffc9a a3=0 items=0 ppid=429 pid=4987 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none comm="cron" exe="/usr/sbin/cron" subj=0:63:0:0 key=(null)` `type=PROCTITLE msg=audit(1712820601.957:21458): proctitle=2F7573722F7362696E2F43524F4E002D66` В соответствии с алгоритмом в этом случае мы получим одно однострочное событие с типом LOGIN, так как тип LOGIN имеет он меньше AUDIT_FIRST_EVENT равного 1300, и одно многострочное событие с SYSCALL и PROCTITLE. При группировке многострочного события auditd, содержащего записи с разными префиксами, в итоговом событии будет исп префикс той записи, которая пришла первой. Это необходимо для корректного парсинга события нормализатором. Например обработки получены следующие записи: `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE msg=audit(1742441361.524:787467): proctitle=686170726F7879002D57002D6462002D66002F7573722F6C6F63616C2F6574632F686170726F78792F686170726F7` `<182>2025-03-20T06:29:22.643145+03:00 test-server-01 tag_audit_log: type=SOCKADDR msg=audit(1742441361.524:787467): saddr=020026FC0A5E41E80000000000000000` `<182>2025-03-20T06:29:22.643143+03:00 test-server-01 tag_audit_log: type=SYSCALL msg=audit(1742441361.5 arch=c000003e syscall=42 success=no exit=-115 a0=1b a1=55d3f02e8c80 a2=10 a3=55d3eec440d0 items=0 ppid= pid=1356 auid=4294967295 uid=99 gid=99 euid=99 suid=99 fsuid=99 egid=99 sgid=99 fsgid=99 tty=(none) ses comm="haproxy" exe="/usr/local/sbin/haproxy" subj=docker-default key="network_events"<` Поскольку первой пришла запись `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE msg=audit(...)`, то в итоговом событии будет использоваться префикс `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log:`. При группировке событий решение игнорирует строки с типом `EOE` (например, `type=EOE msg=audit(1633859647.072:1206` поскольку они не передают важной для событий информации.
Разделитель	Символ, определяющий границу между событиями: • **\n**; • **\t**; • **\0**. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. Это значит, что не будет парсить одно событие на несколько, а передаст в нормализатор как есть.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Количество обработчиков	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
TTL буфера событий	Время жизни буфера для строк событий auditd в миллисекундах. Строки событий auditd попадают в коллектор Kaspersky SIEM Cloud и накапливаются в буфере. Это позволяет сгруппировать несколько строк событий auditd в одно событие auditd. Отсчет времени жизни буфера начинается при получении первой строки события auditd или при истечении предыдущего времени жизни буфера. Доступные значения: от 50 до 30 000. Значение по умолчанию: `2000`. Это поле доступно, если вы включили переключатель **Auditd** на вкладке **Основные параметры**. Строки событий auditd, накопленные в буфере, хранятся в оперативной памяти сервера. Мы рекомендуем с осторожностью увеличивать размер буфера, так как это может привести к использованию слишком большого количества оперативной памяти сервера коллектором Kaspersky SIEM Cloud. Вы можете просмотреть в метриках Kaspersky SIEM Cloud, сколько оперативной памяти сервера использует коллектор Kaspersky SIEM Cloud. Если вы хотите, чтобы время жизни буфера составляло более 30 000 миллисекунд, мы рекомендуем использовать другой транспорт доставки событий auditd. Например, вы можете использовать агента или предварительно накапливать события auditd в файле, после чего обрабатывать файл коллектором Kaspersky SIEM Cloud.
Заголовок транспорта	Регулярное выражение для событий auditd, по которому определяются строки событий auditd. Вы можете использовать значение по умолчанию или изменить его. Регулярное выражение должно содержать группы `record_type_name`, `record_type_value` и `event_sequence_number`. Если многострочное событие auditd содержит префикс, для первой строки события auditd префикс сохраняется, а для последующих – отбрасывается. Вы можете вернуться регулярному выражению для событий auditd по умолчанию, нажав на кнопку **Установить значение по умолчанию**.
Сжатие	Определяет метод распаковки данных, поступающих в коннектор. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.

Коннектор, тип netflow

Коннекторы с типом **netflow** используются для пассивного получения событий в формате NetFlow. Доступные параметры коннектора с типом **netflow** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **netflow**. Обязательный параметр.

Параметр	Описание
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Поддерживаются следующие форматы URL-адресов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address><port number>`. IPv6-адреса можно указать в формате `[<IPv6 address>%<interface>:<port number>`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Вы можете добавить несколько URL-адресов и удалить URL-адрес. Kaspersky SIEM Cloud не позволяет сохранить ресурс или сервис если в поле URL есть знак табуляции или пробел. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Количество обработчиков	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Коннектор, тип sflow

Коннекторы с типом **sflow** используются для пассивного получения событий в формате sFlow. Для sFlow поддерживаются только структуры, описанные в sFlow version 5.

При получении событий в формате sFlow в Kaspersky SIEM Cloud доступна дополнительная нормализация.

Доступные параметры коннектора с типом **sflow** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **sflow**. Обязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Вы можете ввести URL-адрес в одном из следующих форматов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address>:<port number>`; • `:<port number>`. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Количество обработчиков	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Коннектор, тип nats-jetstream

Коннекторы с типом **nats-jetstream** используются для взаимодействия с брокером сообщений NATS при работе с агентами Windows и Linux. Доступные параметры коннектора с типом **nats-jetstream** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **nats-jetstream**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Поддерживаются следующие форматы URL-адресов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address><port number>`. IPv6-адреса можно указать в формате `[<IPv6 address>%<interface>:<port number>`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Вы можете добавить несколько URL-адресов и удалить URL-адрес. Kaspersky SIEM Cloud не позволяет сохранить ресурс или сервис если в поле URL есть знак табуляции или пробел. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр.

Параметр	Описание
Авторизация	Тип авторизации при подключении к URL-адресу, указанному в поле **URL**. • **Выключена**. Это значение выбрано по умолчанию. • **Обычная**. Этот тип авторизации осуществляется с помощью механизма SASL/PLAIN, который передает имя пользователя и пароль в открытом виде. Как правило, для обеспечения безопасности передачи данных (шифрования) в SASL/PLAIN используется TLS. При выборе этого значения в раскрывающемся списке **Секрет** укажите секрет, содержащий учетные данные пользователя для авторизации при подключении к точке назначения. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать секрет?** *Чтобы создать секрет:* 1. В поле **Название** введите название секрета. 2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору. 3. При необходимости в поле **Описание** введите описание секрета. 4. Нажмите на кнопку **Создать**. Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**.
Тема	Тема сообщений NATS. Символы вводятся в кодировке Unicode. Обязательный параметр.
Идентификатор группы	Значение параметра `GroupID` для сообщений NATS. Максимальная длина значения: до 255 символов в кодировке Unicode. Значение по умолчанию: `default`.
Разделитель	Символ, определяющий границу между событиями: • **\n**; • **\t**; • **\0**. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Количество обработчиков	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Параметр	Описание

Режим TLS	Режим шифрования TLS. При использовании шифрования TLS вы не можете указать IP-адрес в поле **URL** на вкладке **Основные параметры**. Доступные значения:
	• **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию.
	• **Включено** – использовать шифрование TLS, но без верификации сертификатов.
	• **Нестандартный CA** – использовать шифрование TLS с верификацией сертификата, подписанного центром сертификации. При выборе этого значения в раскрывающемся списке **Нестандартный CA** укажите секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать сертификат, подписанный центром сертификации?
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра Kaspersky SIEM Cloud (в примерах команд ниже используется OpenSSL).
	Чтобы создать сертификат, подписанный центром сертификации:
	1. Создайте ключ, который будет использоваться центром сертификации, например:
	`openssl genrsa -out ca.key 2048`
	2. Создайте сертификат для созданного ключа, например:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<common name of the certification authority host>" -out ca.crt`
	3. Создайте приватный ключ и запрос на его подписание в центре сертификации, например:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<common host name of the Kaspersky SIEM Cloud server>" -out server.csr`
	4. Создайте сертификат, подписанный центром сертификации. Вам нужно включить в переменную `subjectAltName` доменные имена или IP-адреса сервера, для которого вы создаете сертификат, например:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Загрузите созданный сертификат `server.crt` в веб-интерфейсе Kaspersky SIEM Cloud в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	Для использования сертификатов Kaspersky SIEM Cloud на сторонних устройствах вам нужно изменить расширение файла сертификата с CERT на CRT. В противном случае вы можете получить ошибку `x509: certificate signed by unknown authority`.
	• **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс Kaspersky SIEM Cloud в виде PFX-секрета. При выборе этого значения в раскрывающемся списке **PFX секрет** укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать PFX-секрет?
	Чтобы создать PFX-секрет:
	1. В поле **Название** введите название PFX-секрета.
	2. Нажмите на кнопку **Загрузить PFX** и выберите файл в формате PKCS#12-контейнера, в который вы экспортировали файл PFX с закрытым ключом.
	3. В поле **Пароль** введите пароль для защиты файла PFX, указанный в мастере экспорта PFX.
	4. Нажмите на кнопку **Создать**.
	PFX-секрет будет создан и отобразится в раскрывающемся списке **PFX секрет**.
	Режим **Нестандартный PFX** не отображается, если для параметра **Авторизация** выбрано значение **Обычная**.

Сжатие	Определяет метод распаковки данных, поступающих в коннектор. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.

Коннектор, тип kafka

Коннекторы с типом **kafka** используются для коммуникации с шиной данных Apache Kafka при работе с агентами Windows и Linux. Доступные параметры коннектора с типом **kafka** описаны в таблицах ниже.

С помощью коннектора типа **kafka** Kaspersky SIEM Cloud может принимать события как в несжатом, так и в сжатом виде. Сжатие осуществляется с помощью следующих поддерживаемых **kafka** алгоритмов сжатия: gzip, snappy, zstd и lz4. При поступлении событий в сжатом виде декомпрессия событий происходит автоматически.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **kafka**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Поддерживаются следующие форматы URL-адресов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address><port number>`. IPv6-адреса можно указать в формате `[<IPv6 address>%<interface>:<port number>`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Вы можете добавить несколько URL-адресов и удалить URL-адрес. Kaspersky SIEM Cloud не позволяет сохранить ресурс или сервис если в поле URL есть знак табуляции или пробел. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр.

Параметр	Описание
Авторизация	Тип авторизации при подключении к URL-адресу, указанному в поле **URL**. • **Выключена**. Это значение выбрано по умолчанию. • **Обычная**. Этот тип авторизации осуществляется с помощью механизма SASL/PLAIN, который передает имя пользователя и пароль в открытом виде. Как правило, для обеспечения безопасности передачи данных (шифрования) в SASL/PLAIN используется TLS. При выборе этого значения в раскрывающемся списке **Секрет** укажите секрет, содержащий учетные данные пользователя для авторизации при подключении к точке назначения. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать секрет?** *Чтобы создать секрет:* 1. В поле **Название** введите название секрета. 2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору. 3. При необходимости в поле **Описание** введите описание секрета. 4. Нажмите на кнопку **Создать**. Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**. • **PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать сертификат с закрытым ключом в формате PKCS#12-контейнера во внешнем центре сертификации, экспортировать файл PFX из хранилища, после чего загрузить файл PFX в веб-интерфейс Kaspersky SIEM Cloud в виде PFX-секрета. При выборе этого значения в раскрывающемся списке **PFX секрет** укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать PFX-секрет?** *Чтобы создать PFX-секрет:* 1. В поле **Название** введите название PFX-секрета. 2. Нажмите на кнопку **Загрузить PFX** и выберите файл в формате PKCS#12-контейнера, в который вы экспортировали файл PFX с закрытым ключом. 3. В поле **Пароль** введите пароль для защиты файла PFX, указанный в мастере экспорта PFX. 4. Нажмите на кнопку **Создать**. PFX-секрет будет создан и отобразится в раскрывающемся списке **PFX секрет**. Если для проверки сервера используется цепочка из нескольких сертификатов, для обеспечения правильной очередности сертификатов в цепочке мы рекомендуем собирать файл PFX с помощью OpenSSL. • **SCRAM-SHA-256** – авторизация с помощью защищенного механизма подключения, который использует хеш SHA256 для безопасной проверки подлинности и предотвращает перехват данных. • **SCRAM-SHA-512** – авторизация с помощью защищенного механизма подключения, который использует хеш SHA512 для безопасной проверки подлинности и предотвращает перехват данных. При выборе **SCRAM-SHA-256** или **SCRAM-SHA-512** в качестве типа авторизации в раскрывающемся списке **Секрет** укажите секрет с паролем для авторизации. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета в раскрывающемся списке **Секрет** выберите значение **Создать**.
Топик	Тема сообщений Kafka. Максимальная длина сообщения составляет 255 символов. Недопустимо использование символов пробела и табуляции. Вы можете использовать следующие символы: a–z, A–Z, 0–9, ".", "_", "-". Обязательный параметр.
Идентификатор группы	Значение параметра `GroupID` для сообщений Kafka. Максимальная длина значения: 255 символов. Вы можете использовать символы a–z, A–Z, 0–9, ".", "_", "-".
Разделитель	Символ, определяющий границу между событиями: • **\n**; • **\t**; • **\0**. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Количество обработчиков	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999. По умолчанию количество обработчиков равно 256.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Режим TLS	Режим шифрования TLS. При использовании шифрования TLS вы не можете указать IP-адрес в поле **URL** на вкладке **Основные параметры**. Доступные значения:
	• **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию.
	• **Включено** – использовать шифрование TLS, но без верификации сертификатов.
	• **Нестандартный CA** – использовать шифрование TLS с верификацией сертификата, подписанного центром сертификации. При выборе этого значения в раскрывающемся списке **Нестандартный CA** укажите секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать сертификат, подписанный центром сертификации?
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра Kaspersky SIEM Cloud (в примерах команд ниже используется OpenSSL).
	Чтобы создать сертификат, подписанный центром сертификации:
	1. Создайте ключ, который будет использоваться центром сертификации, например:
	`openssl genrsa -out ca.key 2048`
	2. Создайте сертификат для созданного ключа, например:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<common name of the certification authority host>" -out ca.crt`
	3. Создайте приватный ключ и запрос на его подписание в центре сертификации, например:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<common host name of the Kaspersky SIEM Cloud server>" -out server.csr`
	4. Создайте сертификат, подписанный центром сертификации. Вам нужно включить в переменную `subjectAltName` доменные имена или IP-адреса сервера, для которого вы создаете сертификат, например:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Загрузите созданный сертификат `server.crt` в веб-интерфейсе Kaspersky SIEM Cloud в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	Для использования сертификатов Kaspersky SIEM Cloud на сторонних устройствах вам нужно изменить расширение файла сертификата с CERT на CRT. В противном случае вы можете получить ошибку `x509: certificate signed by unknown authority`.

Размер одного сообщения в запросе	Размер одного сообщения в запросе в байтах. Значение по умолчанию: 16 МБ, применяется если значение не указано или указано 0. Значение не может быть больше 2147483647 байт.
Максимальное время ожидания одного сообщения	Время ожидания одного сообщения в секундах. Значение по умолчанию: 5 секунд, применяется если значение не указано или указано 0. Максимально допустимое значение= 2147483647.
Время ожидания подключения	Время ожидания установки соединения с брокером Kafka в секундах. Максимально допустимое значение: 2147483647. По умолчанию 30 секунд.
Время ожидания чтения	Время ожидания операции чтения в секундах. Максимально допустимое значение: 2147483647. По умолчанию 30 секунд.
Время ожидания записи	Время ожидания операции записи в секундах. Максимально допустимое значение: 2147483647. По умолчанию 30 секунд.

Параметр	Описание
Интервал обновления состояния группы	Интервал обновления состояния группы в секундах. Интервал обновления не может превышать время сессии. Рекомендуемое значение: 1/3 от времени сессии. Максимально допустимое значение: 2147483647. По умолчанию 3 секунды.
Время сессии	Время сессии в секундах. Максимально допустимое значение: 2147483647. По умолчанию 10 секунд.
Максимальное время обработки одного сообщения	Максимальное время обработки одного сообщения одним потоком в миллисекундах. Максимально допустимое значение: 2147483647. По умолчанию 100 миллисекунд.
Включить автокоммит	По умолчанию включено.
Интервал автокоммита	Интервал автокоммита в секундах. По умолчанию 1 секунда. Максимально допустимое значение: 18446744073709551615. Можно указать любое положительное число.

Коннектор, тип http

Коннекторы с типом **http** используются для получения событий по протоколу HTTP при работе с агентами Windows и Linux. Доступные параметры коннектора с типом **http** описаны в таблицах ниже.

С помощью коннектора типа **http** Kaspersky SIEM Cloud может принимать события как в несжатом, так и в сжатом виде. При поступлении событий в сжатом виде, например событий Kaspersky Endpoint Security for Windows, декомпрессия событий происходит автоматически.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **http**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Вы можете ввести URL-адрес в одном из следующих форматов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address>:<port number>`; • `:<port number>`. Для того чтобы данные из источника событий отправлялись в коннектор, указанный вами URL-адрес должен оканчиваться на `/input`. Обязательный параметр.

Параметр	Описание
Разделитель	Символ, определяющий границу между событиями: • \n; • \t; • \0. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
Режим TLS	Режим шифрования TLS. При использовании шифрования TLS вы не можете указать IP-адрес в поле URL на вкладке **Основные параметры**. Доступные значения: • **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию. • **Включено** – использовать шифрование TLS, но без верификации сертификатов. • **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс Kaspersky SIEM Cloud в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение Создать. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать PFX-секрет?** *Чтобы создать PFX-секрет:* 1. В поле **Название** введите название PFX-секрета. 2. Нажмите на кнопку **Загрузить PFX** и выберите файл в формате PKCS#12-контейнера, в который вы экспортировали файл PFX с закрытым ключом. 3. В поле **Пароль** введите пароль для защиты файла PFX, указанный в мастере экспорта PFX. 4. Нажмите на кнопку **Создать**. PFX-секрет будет создан и отобразится в раскрывающемся списке **PFX секрет**. • **Нестандартный PFX с аутентификацией клиента** – использовать шифрование TLS с PFX-секретом. В этом режиме выполняется аутентификация клиента по сертификату. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс Kaspersky SIEM Cloud в виде PFX-секрета. При выборе этого значения в раскрывающемся списке PFX секрет укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение Создать. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать PFX-секрет?** *Чтобы создать PFX-секрет:* 1. В поле **Название** введите название PFX-секрета. 2. Нажмите на кнопку **Загрузить PFX** и выберите файл в формате PKCS#12-контейнера, в который вы экспортировали файл PFX с закрытым ключом. 3. В поле **Пароль** введите пароль для защиты файла PFX, указанный в мастере экспорта PFX. 4. Нажмите на кнопку **Создать**. PFX-секрет будет создан и отобразится в раскрывающемся списке **PFX секрет**.

Коннектор, тип sql

Коннекторы с типом **sql** используются для выборки данных из СУБД. Kaspersky SIEM Cloud поддерживает работу с несколькими типами баз данных.

Поддерживаемые типы баз данных

Решение поддерживает работу со следующими типами баз данных SQL:

- SQLite.
- MariaDB 10.5 и выше.
- MsSQL.
- MySQL 5.7 и выше.
- PostgreSQL.
- Cockroach.
- Oracle.
- Firebird.

При создании коннектора с типом **sql** вам нужно указать значения для общих параметров коннектора и отдельных параметров подключения к базе данных. Доступные параметры коннектора с типом **sql** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **sql**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Запрос по умолчанию	SQL-запрос, который выполняется при подключении к базе данных. Обязательный параметр.
Переподключаться к БД каждый раз при отправке запроса	Переключатель, включающий переподключение коннектора к базе данных при отправке запроса. По умолчанию этот переключатель выключен.
Интервал запросов, сек.	Интервал выполнения SQL-запросов в секундах. Значение по умолчанию: 10 секунд.

<table>
<tr><th>Параметр</th><th>Описание</th></tr>
<tr><td>Соединение</td><td>Параметры в этом блоке зависят от выбранного типа базы данных для подключения:
MySQL
MSSQL
Postgres
SQLite3
Oracle
Firebird
ClickHouse
ODBC
Тип базы данных – тип базы данных для подключения. При выборе типа базы данных в поле URL отображается префикс, соответствующий протоколу взаимодействия. Например, для типа базы данных ClickHouse в поле URL отображается префикс <code>clickhouse://</code>.
Секрет отдельно – флажок, позволяющий просматривать информацию о подключении. Если вы установили флажок Секрет отдельно, учетные данные задаются в поле Секрет, а строка подключения вводится в поле URL без указания учетных данных пользователя.
URL – URL-адрес подключения. Если вы установили флажок Секрет отдельно, вы сможете указать URL без учетных данных пользователя (логина и пароля пользователя), и потом задать эти данные в отдельном поле Секрет. Если флажок Секрет отдельно не установлен, в этом поле нужно выбрать секрет urls, внутри которого нужно указать URL подключения вместе с учетными данными пользователя (логин и пароль пользователя).
При создании подключений, если информация о подключении задана в секрете urls, могут неправильно обрабатываться строки с учетными данными, содержащими специальные символы. Если при создании подключения возникает ошибка, но вы уверены в том, что указали правильные значения параметров, укажите специальные символы в процентной кодировке.
Коды специальных символов<table><tr><td>!</td><td>#</td><td>$</td><td>%</td><td>&</td><td>'</td><td>(</td><td>)</td><td>*</td><td>+</td></tr><tr><td>%21</td><td>%23</td><td>%24</td><td>%25</td><td>%26</td><td>%27</td><td>%28</td><td>%29</td><td>%2A</td><td>%2B</td></tr><tr><td>.</td><td>/</td><td>:</td><td>;</td><td>=</td><td>?</td><td>@</td><td>[</td><td>]</td><td>\</td></tr><tr><td>%2C</td><td>%2F</td><td>%3A</td><td>%3B</td><td>%3D</td><td>%3F</td><td>%40</td><td>%5B</td><td>%5D</td><td>%5C</td></tr></table>Следующие специальные символы не поддерживаются в паролях доступа к базам SQL: пробел, [,], :, /, #, %, \.
Если вы установили флажок Секрет отдельно, кодирование специальных символов не требуется.
Если вы хотите изменить параметры существующего URL-адреса, нажмите рядом с ним на значок карандаша .
Секрет – секрет credentials, в котором хранится список URL-адресов для подключения к базе данных. Это поле отображается, если вы установили флажок Секрет отдельно.
Столбец идентификатора – название столбца, содержащего идентификатор для каждой строки таблицы. Обязательный параметр.
Начальное значение идентификатора – значение в столбце идентификатора для определения строки, с которой требуется начать считывание данных из SQL-таблицы.
Запрос – дополнительный SQL-запрос, который выполняется вместо SQL-запроса по умолчанию.
Интервал запросов, сек – интервал выполнения SQL-запросов в секундах. Указанный интервал используется вместо интервала, указанного по умолчанию для коннектора. Значение по умолчанию: 10 секунд.
Вы можете добавить несколько подключений или удалить подключение. Для добавления подключения нажмите на кнопку + Добавить подключение. Для удаления подключения нажмите рядом с ним на значок удаления ✕.</td></tr>
<tr><td>Описание</td><td>Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.</td></tr>
</table>

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**. Kaspersky SIEM Cloud конвертирует ответы SQL в кодировку UTF-8. Вы можете настроить SQL-сервер на отправку ответов в кодировке UTF-8 или выбрать их кодировку на стороне Kaspersky SIEM Cloud.

В рамках одного коннектора вы можете **создать подключение** для нескольких поддерживаемых баз данных. Если коллектор с коннектором типа **sql** не удается запустить, вам нужно проверить, пуст ли state-файл /opt/kaspersky/kuma/collector/<collector ID>/sql/state-<file ID>. Если state-файл пуст, вам нужно его удалить и перезапустить коллектор.

Чтобы создать подключение для нескольких баз данных SQL:

1. Нажмите на кнопку **Добавить подключение**.
2. Задайте значение для параметров **URL**, **Столбец идентификатора**, **Начальное значение идентификатора**, **Запрос**, **Интервал запросов, сек**.
3. Повторите шаги 1–2 для каждого требуемого подключения.

Поддерживаемые типы SQL и особенности их использования

Поддерживаются следующие типы SQL:

- MSSQL.

  Например:

  - `sqlserver://{user}:{password}@{server:port}/{instance_name}?database={database}`

  Мы рекомендуем использовать этот вариант URL.

  - `sqlserver://{user}:{password}@{server}?database={database}`

  В качестве плейсхолдера в SQL-запросе используются символы `@p1`.

  > Если вы хотите подключиться с доменными учетными данными, укажите имя учетной записи в формате `<domain>%5C<user>`. Например: `sqlserver://domain%5Cuser:password@ksc.example.com:1433/SQLEXPRESS?database=KAV`.

- MySQL/MariaDB.

  Например:

  `mysql://{user}:{password}@tcp({server}:{port})/{database}`

  В качестве плейсхолдера в SQL-запросе используются символ `?`.

- PostgreSQL.

  Например: `postgres://{user}:{password}@{server}/{database}?sslmode=disable`

  В качестве плейсхолдера в SQL-запросе используются символы `$1`.

- CockroachDB.

  Например:

  `postgres://{user}:{password}@{server}:{port}/{database}?sslmode=disable`

  В качестве плейсхолдера в SQL-запросе используются символы `$1`.

- SQLite3.

  Например:

  `sqlite3://file:{file_path}`

В качестве плейсхолдера в SQL-запросе используется знак вопроса: `?`.

При обращении к SQLite3, если начальное значение идентификатора используется в формате datetime, вам нужно добавить преобразование даты с помощью функции `sqlite datetime` в SQL-запрос. Например:

```
select * from connections where datetime(login_time) > datetime(?, 'utc') order by login_time
```

В этом примере `connections` – это таблица SQLite, а значение переменной `?` берется из поля **Начальное значение идентификатора**, и его требуется указывать в формате `{<date>}T{<time>}Z`, например `2021-01-01T00:10:00Z)`.

- Oracle DB.

  Пример URL секрета с драйвером oracle:

  ```
  oracle://{user}:{password}@{server}:{port}/{service_name}
  ```

  ```
  oracle://{user}:{password}@{server}:{port}/?SID={SID_VALUE}
  ```

  Если время выполнения запроса превышает 30 секунд. драйвер oracle прерывает SQL-запрос и в журнале коллектора появится ошибка **user requested cancel of current operation**. Для увеличения времени выполнения SQL-запроса укажите в строке подключения значение параметра **timeout** в секундах, например:

  ```
  oracle://{user}:{password}@{server}:{port}/{service_name}?timeout=300
  ```

  В качестве плейсхолдера в SQL-запросе используется переменная `:val`.

  При обращении к Oracle DB, если начальное значение идентификатора используется в формате datetime, требуется учитывать тип поля в базе данных и при необходимости добавить дополнительные преобразования строки со временем в SQL-запросе для обеспечения правильной работы SQL-коннектора. Например, если в базе создана таблица `Connections`, в которой есть поле `login_time`, возможны следующие преобразования:

  - Если у поля **login_time** тип TIMESTAMP, в зависимости от параметров базы данных в поле **login_time** может быть указано значение в формате `YYYY-MM-DD HH24:MI:SS`, например `2021-01-01 00:00:00`. В этом случае вам нужно указать значение `2021-01-01T00:00:00Z` в поле **Начальное значение идентификатора**, а в SQL-запросе произвести преобразование с помощью функции `to_timestamp`, например:

    ```
    select * from connections where login_time > to_timestamp(:val, 'YYYY-MM-DD"T"HH24:MI:SS"Z"')
    ```

  - Если у поля **login_time** тип TIMESTAMP WITH TIME ZONE, в зависимости от параметров базы данных в поле **login_time** может быть указано значение в формате `YYYY-MM-DD"T"HH24:MI:SSTZH:TZM`, например `2021-01-01T00:00:00+03:00`. В этом случае вам нужно указать значение `2021-01-01T00:00:00+03:00` в поле Начальное значение идентификатора, а в SQL-запросе произвести преобразование с помощью функции `to_timestamp_tz`, например:

    ```
    select * from connections_tz where login_time > to_timestamp_tz(:val, 'YYYY-MM-DD"T"HH24:MI:SSTZH:TZM')
    ```

    Подробнее о функциях `to_timestamp` и `to_timestamp_tz` см. в официальной документации Oracle.

  Для обращения к Oracle DB вам нужно установить пакет Astra Linux libaio1.

- Firebird® SQL.

  Например:

  ```
  firebirdsql://{user}:{password}@{server}:{port}/{database}
  ```

  В качестве плейсхолдера в SQL-запросе используется знак вопроса: `?`.

Если возникает проблема подключения к firebird на Windows, используйте полный путь до файла с базой данных, например:

`firebirdsql://{user}:{password}@{server}:{port}/C:\Users\user\firebird\db.FDB`

- ClickHouse.

  Например:

  `clickhouse://{user}:{password}@{server}:{port}/{database}`

  В качестве плейсхолдера в SQL-запросе используется знак вопроса: `?`.

  Kaspersky SIEM Cloud поддерживает работу со следующими типами данных:

  - Данные, которые можно привести к строковому формату (например, строки, числовые значения и BLOB-объекты), отображаются в виде строк.
  - Массивы данных и карты отображаются в формате JSON или с помощью встроенного механизма go `fmt.Sprintf("%v",v)` показываются оптимальным доступным образом.

  Подключение к ClickHouse может осуществляться двумя способами:

  - Без использования учетных данных: необходимо ввести URL-адрес `clickhouse://host:port/database`.
  - С учетными данными: требуется использовать URL-адрес `clickhouse://user:password@host:port/database`.

  При использовании шифрования TLS по умолчанию коннектор работает только по порту 9440. Если шифрование TLS не используется, по умолчанию коннектор работает с ClickHouse только по порту 9000.

  > Коннектор не работает по протоколу http.

  Если на сервере с ClickHouse настроен режим шифрования TLS, а в параметрах коннектора в раскрывающемся списке **Режим TLS** выбрано **Выключено** или наоборот, соединение с базой данных не будет установлено.

  > **Режим TLS** используется только если указан драйвер ClickHouse.

  Если вы хотите подключиться к ClickHouse Kaspersky SIEM Cloud, вам нужно в параметрах коннектора с типом **SQL** указать тип секрета **PublicPKI**, который содержит закрытый ключ PEM, закодированный в base64, и открытый ключ.

  В параметрах коннектора с типом **SQL** для типа соединения ClickHouse вам нужно выбрать **Выключено** в раскрывающемся списке **Режим TLS**. Это значение недопустимо указывать, если для аутентификации используется сертификат. Если в раскрывающемся списке **Режим TLS** вы выбираете **Нестандартный CA**, в поле **Секрет** вам нужно указать ID секрета типа certificate. Вам также нужно выбрать одно из следующих значений в раскрывающемся списке **Тип авторизации**:

  - **Выключено**. При выборе этого значения вам нужно оставить пустым значение в поле **Секрет**.
  - **Обычная**. Вам нужно выбрать это значение, если установлен флажок **Секрет отдельно** и в поле **Секрет** указан ID секрета типа credentials.
  - **PublicPKI**. Вам нужно выбрать это значение, если установлен флажок **Секрет отдельно** и в поле **Секрет** указан ID секрета типа PublicPKI.

Если в начальном значении идентификатора есть указание времени (`datetime`), в запросе необходимо ввести переменную для преобразования времени (`parseDateTimeBestEffort`). Например, если время указано как `2021-01-01 00:10:00`, то запрос будет следующим:

```
select connections, username, host, login_time from connections where login_time >
parseDateTimeBestEffort(?) order by login_time
```

- ODBC.

  Например:

  `odbc://{server}:{port}/{database}` – если вы установили флажок **Секрет отдельно** при настройке параметров соединения.

  `odbc://{user}:{password}@{server}:{port}/{database}` – если вы установили флажок **Секрет отдельно** при настройке параметров соединения.

  `odbc://{server}:{port}/{database}?params1=value1&params2=value2` – если вам нужно указать все параметры соединения.

  В качестве плейсхолдера в SQL-запросе используется знак вопроса: `?`.

  > ODBC не поддерживается, когда коллектор развертывается в Kubernetes.

  Если вы используете ODBC, вам нужно указать имя драйвера базы данных ODBC для параметра **Имя файла драйвера ODBC**. Затем файл драйвера нужно сохранить в директории `/opt/kaspersky/kuma/collector/<uuid_of_collector>/driver`.

  > Решение использует системную утилиту для управления ODBC-драйверами и подключениями к базам данных ODBC Manager версии 2.3.14. Вам нужно использовать ODBC-драйверы, совместимые с этой версией системной утилиты.

  При указании имени драйвера базы данных ODBC нужно учитывать следующее:

  - Если у драйвера есть зависимости, их нужно сохранить в директории `/opt/kaspersky/kuma/collector/<uuid_of_collector>/driver` или `/opt/kaspersky/kuma/collector/<uuid_of_collector>/` (если этого требует драйвер).
  - Параметр чувствителен к регистру.
  - При указании путей допускается использование специальных символов.

  Пример имени драйвера базы данных ODBC

  ```
  psqlodbcw.so
  ```

  Для использования SQL-коннектора типа ODBC в существующем коллекторе после обновления решения вам нужно удалить, а затем повторно установить этот коллектор. Это позволит получить значения всех переменных окружения, которые нужны для правильной работы коннектора типа ODBC.

  Пример настройки SQL-коннектора с ODBC-драйвером

Чтобы настроить параметры коннектора для работы с ODBC-драйвером (на примере ODBC-драйвера для PostgreSQL и ОС Astra):

1. Уточните, есть ли ODBC для интересующей вас базы данных. Если такой драйвер существует, найдите в Интернет название файла с этим драйвером с расширением .so.

2. В разделе **Ресурсы** → **Коннекторы** создайте SQL-коннектор, в поле **Тип базы данных** выбрав **ODBC**.

3. Заполните все обязательные поля для нового коннектора, указав в поле **Имя файла драйвера ODBC** имя ODBC-драйвера.

   При необходимости вы сможете изменить имя драйвера после установки коллектора с указанным коннектором.

4. Установите коллектор с SQL-коннектором на хосте.

5. Скачайте необходимый файл с расширением .so. Если вы работаете с базой данных для PostgreSQL, вы можете скачать этот файл с помощью следующей команды:

   ```
   apt download odbc-postgresql
   ```

   Решение скачает deb-пакет `ibpq5_15.17-astra.se2.3r2_amd64.deb` для ОС Astra.

6. Выполните следующие действия:

   a. Распакуйте `ibpq5_15.17-astra.se2.3r2_amd64.deb`, выполнив следующую команду:

   ```
   ar x libpq5_15.17-astra.se2.3r2_amd64.deb
   ```

   b. Распакуйте архив `data.tar.xz` с помощью следующей команды:

   ```
   tar -xf data.tar.xz
   ```

7. В распакованных файлах найдите файлы с расширением .so, выполнив следующую команду:

   ```
   find . -name ".so"
   ```

8. Скопируйте ODBC-драйвер для PostgreSQL в директорию `driver`, которая находится в папке коллектора с помощью следующей команды:

   ```
   cp ./usr/lib/x86_64-linux-gnu/odbc/psqlodbcw.so /opt/kaspersky/kuma/collector/<ID>/driver/psqlodbcw.so
   ```

9. Проверьте, все ли зависимости ODBC-драйвера есть на хосте, выполнив следующую команду:

```
LD_LIBRARY_PATH="/opt/kaspersky/kuma/collector/<ID>/deps/odbc:/opt/kaspersky/kuma/collector/<ID>/driver"
ldd /opt/kaspersky/kuma/collector/<ID>/driver/psqlodbcw.so | grep "not found"
```

где `<ID>` – идентификатор установленного коллектора.

Если в результате выполнения команды отображается `libpq.so.5 => not found`, вам нужно дополнительно скачать зависимость `libpq.so.5`. Для ОС Astra это также можно сделать, выполнив команду:

```
apt download libpq5
```

После этого распакуйте deb-пакет и выполните поиск файла с расширением .so. Найденный файл с расширением .so нужно переместить в директорию `driver` в папке коллектора (`cp ./usr/lib/x86_64-linux-gnu/libpq.so.5.15 /opt/kaspersky/kuma/collector/<ID>/driver/libpq.so.5`).

10. Повторно проверьте наличие всех зависимостей ODBC-драйвера на хосте. Также убедитесь в том, что название файла с драйвером в директории `driver` коллектора (`/opt/kaspersky/kuma/collector/<ID>/driver/psqlodbcw.so`) соответствует названию файла в конфигурационном файле.

Чтобы провести диагностику и убедиться, что недостающие зависимости отсутствуют, вы можете добавить в systemd-файл коллектора строку `- Environment=LD_DEBUG=libs` и выполнить следующую команду:

```
systemctl daemon-reload
```

Затем вам нужно повторно запустить коллектор и в журнале `journalctl` отобразится информация о поиске зависимостей ODBC-драйвером.

Для каждого вида ODBC-драйвера существуют особенности представления данных о недостающих зависимостях. Например, ODBC-драйвер MsSQL ищет зависимости на уровень выше директории `driver`. Вам нужно сохранить недостающую папку `share` в `/opt/kaspersky/kuma/collector/<ID>`, а не в директории `driver`. Также могут быть особенности указания URL для разных ODBC-драйверов. Например, для ODBC-драйвера Oracle вам нужно указать URL в конфигурационном файле коннектора в формате `odbc://?DBQ=//{server}:{port}/{database}` (при этом при этом логин и пароль пользователя указываются в секрете credentials в поле **Секрет**, если вы установили флажок **Секрет отдельно**).

> При настройке параметров ODBC-драйвера мы рекомендуем руководствоваться документацией конкретного драйвера.

11. Перезапустите коллектор.

В SQL-запросах поддерживается последовательный запрос сведений из базы данных. Например, если в поле **Запрос** указать SQL-запрос `select * from <data table name> where id > <placeholder>`, при первом обращении к таблице в качестве значения плейсхолдера будет использоваться значение поля **Начальное значение идентификатора**. При этом в сервисе, в котором используется SQL-коннектор, сохраняется идентификатор последней прочитанной записи, и во время следующего обращения к базе данных в качестве значения плейсхолдера в запросе будет использоваться идентификатор этой записи.

> В строку запроса рекомендуется добавлять команду `order by`, после которой указывается поле для сортировки. Например, `select * from table_name where id > ? order by id`.

Примеры SQL-запросов

SQLite, Firebird, MySQL, MariaDB, ClickHouse, ODBC – `select * from table_name where id > ? order by id`

MSSQL – `select * from table_name where id > @p1 order by id`

PostgreSQL, Cockroach – `select * from table_name where id > $1 order by id`

Oracle – `select * from table_name where id > :val order by id`

Коннектор, тип file

Коннекторы с типом **file** используются для получения данных из текстовых файлов при работе с агентами Windows и Linux. Одна строка текстового файла считается одним событием. В качестве разделителя строк используется `\n`.

Если при создании коллектора на шаге Транспорт мастера установки вы указали коннектор с типом **file**, на шаге **Парсинг событий** в таблице **Сопоставление** вы можете передать в поле события Kaspersky SIEM Cloud название обрабатываемого коллектором файла или путь к файлу. Для этого в столбце **Исходные данные** укажите одно из следующих значений:

- `$kuma_fileSourceName` – передать в поле события Kaspersky SIEM Cloud название обрабатываемого коллектором файла.
- `$kuma_fileSourcePath` – передать в поле события Kaspersky SIEM Cloud путь к обрабатываемому коллектором файлу.

Когда вы используете коннектор с типом **file**, новые переменные в нормализаторе будут работать только с точками назначения с типом internal.

Для чтения Windows-файлов вам нужно создать коннектор с типом **file** и установить агент на Windows вручную. Windows-агент не должен читать свои файлы в папке, где установлен агент. Коннектор будет работать, даже если файловая система FAT: если дефрагментировать диск, коннектор перечитает все файлы с начала, так все inode файлов сбрасываются.

> Мы не рекомендуем запускать агент под учетной записью администратора; необходимо, чтобы права чтения на папки/файлы были настроены для учетной записи агента. Мы не рекомендуем ставить агент на важные системы, лучше пересылать журналы и читать их на отдельных хостах с агентом.

Для каждого файла, с которым взаимодействует коннектор с типом **file**, создается файл состояния (states.ini) с параметрами `offset`, `dev`, `inode` и `filename`. Файл состояния позволяет коннектору при перечитывании файла возобновлять чтение с места, где коннектор остановился в последний раз, а не начинать чтение заново. Существуют следующие особенности перечитывания файлов:

- Если параметр `inode` в файле состояния изменится, при перечитывании файла, которому соответствует файл состояния, коннектор начнет чтение заново. При удалении и повторном создании файла параметр `inode` в соответствующем файле состояния может не измениться. В этом случае при перечитывании файла коннектор возобновит чтение на основании параметра `offset`.
- Если файл был обрезан или уменьшился его размер, при перечитывании файла коннектор начнет чтение заново.

- Если файл был переименован, при перечитывании файла коннектор возобновит чтение с места, где коннектор остановился в последний раз.

- Если директория с файлом была перемонтирована, при перечитывании файла коннектор возобновит чтение с места, где коннектор остановился в последний раз. Вы можете указать путь к файлам, с которыми взаимодействует коннектор, при настройке коннектора в поле **Путь к файлу**.

Доступные параметры коннектора с типом **file** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **file**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.

Параметр	Описание

Путь к файлу	Коннекторы с типом **file** используются для получения данных из текстовых файлов при работе с агентами Windows и Linux. Одна текстового файла считается одним событием. В качестве разделителя строк используется `\n`.
	
	Полный путь к файлу, с которым коннектор выполняет взаимодействие. Поддерживаются форматы путей как для Linux, так и для например:
	• для Windows: `C:\var\log\test123.log`
	• для Linux: `/var/log/test123.log`
	Недопустимо указывать пути, соответствующие следующим регулярным выражениям:
	• `(?i)^[a-zA-Z]:\\Program Files`
	• `(?i)^[a-zA-Z]:\\Program Files\(x86\)`
	• `(?i)^[a-zA-Z]:\\Windows`
	• `(?i)^[a-zA-Z]:\\ProgramData\\Kaspersky Lab\\KUMA`
	В приведенных регулярных выражениях двойные обратные косые черты (\\) используются системой в качестве части синтаксис регулярного выражения для проверки пути и не должны указываться в самом пути вручную.
	Шаблоны масок для файлов и директорий
	Маски:
	• `'*'` – соответствует любой последовательности символов;
	• `'[' [ '^' ] { < диапазон символов > } ']'` – класс символов (не должен быть пустым);
	• `'?'` – соответствует любому одиночному символу.
	Диапазоны символов:
	• `[0-9]` – числа;
	• `[a-zA-Z]` – буквы латинского алфавита.
	Пример:
	Маски можно использовать как в путях Linux, так и Windows с заменой прямой косой черты на обратную:
	• Для Linux:
	  • `/var/log/*som?[1-9].log`
	  • `/mnt/dns_logs/*/dns.log`
	  • `/mnt/proxy/access*.log`
	• Для Windows:
	  • `C:\var\log\test123.log`
	  • `D:\data\*\report?.txt`
	
	Ограничения при использовании префиксов к путям файлов
	Префиксы, которые невозможно использовать при указании путей к файлам:
	• `/*`
	• `/bin`
	• `/boot`
	• `/dev`
	• `/etc`
	• `/home`
	• `/lib`
	• `/lib64`
	• `/proc`
	• `/root`
	• `/run`
	• `/sys`
	• `/tmp`
	• `/usr/*`

Параметр	Описание

	• `/usr/bin/`
	• `/usr/local/*`
	• `/usr/local/sbin/`
	• `/usr/local/bin/`
	• `/usr/sbin/`
	• `/usr/lib/`
	• `/usr/lib64/`
	• `/var/*`
	• `/var/lib/`
	• `/var/run/`
	• `/opt/kaspersky/kuma/`
	
	Приведенные префиксы используются системой в качестве регулярных выражений для проверки пути. Символ * в префиксах соответствует л последовательности символов и не должен указываться в самом пути вручную, если это не часть допустимого пути.
	
	Файлы по указанным ниже путям доступны:
	
	• `/opt/kaspersky/kuma/clickhouse/logs/`
	• `/opt/kaspersky/kuma/metrics/log/`
	
	Ограничение количества отслеживаемых файлов по маске
	
	Количество одновременно отслеживаемых файлов по маске может быть ограничено параметром Ядра `max_user_watches`. Для просмотра з параметра выполните команду:
	
	`cat /proc/sys/fs/inotify/max_user_watches`
	
	Если количество файлов для отслеживания превышает значение параметра `max_user_watches`, коллектор больше не сможет считывать соб файлов и в журнале коллектора появится следующая ошибка:
	
	`Failed to add files for watching {"error": "no space left on device"}`
	
	Для продолжения правильной работы коллектора вы можете настроить правильную ротацию файлов, чтобы количество файлов не превышал параметра `max_user_watches`, или увеличить значение `max_user_watches`.
	
	Для увеличения значения параметра выполните команду:
	
	`sysctl fs.inotify.max_user_watches=<number of files>`
	
	`sysctl -p`
	
	Вы можете добавить значение параметра `max_user_watches` в sysctl.conf, чтобы значение сохранялось всегда.
	
	После того, как вы увеличите значение параметра `max_user_watches`, коллектор успешно продолжит работу.
	
	Обязательный параметр.

Время ожидания изменений, сек	Время в секундах, в течение которого файл не должен обновляться, чтобы Kaspersky SIEM Cloud выполнила с ним действие, ука раскрывающемся списке **Действие после таймаута**. Значение по умолчанию: `0` – если файл не обновляется, Kaspersky SIEM C выполняет с ним никакого действия. Введенное значение не должно быть меньше значения, которое вы ввели на вкладке **Дополнительные параметры** в поле **Интер запросов, мс**.
Действие после таймаута	Действие, которое Kaspersky SIEM Cloud выполняет с файлом по прошествии времени, указанного в поле **Время ожидания изм сек**: • **Ничего не делать**. Значение по умолчанию. • **Добавление суффикса** – добавить к названию файла расширение .kuma_processed и не обрабатывать файл даже при его с • **Удаление** – удалить файл.

Параметр	Описание
Auditd	Переключатель, включающий механизм auditd, который группирует полученные от коннектора строки событий auditd в одно со auditd. Если вы включили этот переключатель, вы не можете выбрать значение в раскрывающемся списке **Разделитель**, так как для мех auditd автоматически выбирается значение **\n**. Если вы включили этот переключатель в параметрах коннектора агента, вам нужно выбрать значение **\n** в раскрывающемся спи **Разделитель** в параметрах коннектора коллектора, в который агент отправляет события. Максимальный размер сгруппированного события auditd составляет примерно 4 174 304 символов. Kaspersky SIEM Cloud классифицирует события Auditd в соответствии с алгоритмом. Например, для обработки получены сле записи: `type=LOGIN msg=audit(1712820601.957:21458): pid=4987 uid=0 subj=0:63:0:0 old-auid=4294967295 auid=0 tty= old-ses=4294967295 ses=2348 res=1` `type=SYSCALL msg=audit(1712820601.957:21458): arch=c000003e syscall=1 success=yes exit=1 a0=7 a1=7ffc9a0 a3=0 items=0 ppid=429 pid=4987 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) comm="cron" exe="/usr/sbin/cron" subj=0:63:0:0 key=(null)` `type=PROCTITLE msg=audit(1712820601.957:21458): proctitle=2F7573722F7362696E2F43524F4E002D66` В соответствии с алгоритмом в этом случае мы получим одно однострочное событие с типом LOGIN, так как тип LOGIN имеет он меньше AUDIT_FIRST_EVENT равного 1300, и одно многострочное событие с SYSCALL и PROCTITLE. При группировке многострочного события auditd, содержащего записи с разными префиксами, в итоговом событии будет испо префикс той записи, которая пришла первой. Это необходимо для корректного парсинга события нормализатором. Например, обработки получены следующие записи: `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE msg=audit(1742441361.524:787467): proctitle=686170726F7879002D57002D6462002D66002F7573722F6C6F63616C2F6574632F686170726F78792F686170726F78` `<182>2025-03-20T06:29:22.643145+03:00 test-server-01 tag_audit_log: type=SOCKADDR msg=audit(1742441361.524:787467): saddr=020026FC0A5E41E80000000000000000` `<182>2025-03-20T06:29:22.643143+03:00 test-server-01 tag_audit_log: type=SYSCALL msg=audit(1742441361.52 arch=c000003e syscall=42 success=no exit=-115 a0=1b a1=55d3f02e8c80 a2=10 a3=55d3eec440d0 items=0 ppid=1 pid=1356 auid=4294967295 uid=99 gid=99 euid=99 suid=99 fsuid=99 egid=99 sgid=99 fsgid=99 tty=(none) ses= comm="haproxy" exe="/usr/local/sbin/haproxy" subj=docker-default key="network_events"<` Поскольку первой пришла запись `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log: type=PROCTITLE msg=audit(...)`, то в итоговом событии будет использоваться префикс `<182>2025-03-20T06:29:22.643147+03:00 test-server-01 tag_audit_log:`. При группировке событий решение игнорирует строки с типом `EOE` (например, `type=EOE msg=audit(1633859647.072:1206` поскольку они не передают важной для событий информации.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Количество обработчиков	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Режим опроса файла/папки	Режим, в котором коннектор перечитывает файлы в директории: • **Отслеживать изменения** – коннектор перечитывает файлы в директории с интервалом в миллисекундах, указанным в поле **Интервал запросов, мс**, если файлы не обновляются. Значение по умолчанию. Например, если файлы постоянно обновляются, а в поле **Интервал запросов, мс** вы ввели `5000`, коннектор будет перечитывать файлы постоянно, а не с интервалом в 5000 миллисекунд. Если файлы не обновляются, коннектор будет перечитывать их с интервалом в 5000 миллисекунд. • **Отслеживать периодически** – коннектор перечитывает файлы в директории с интервалом в миллисекундах, указанным в поле **Интервал запросов, мс**, вне зависимости от того, обновляются файлы или нет.

Параметр	Описание
Интервал запросов, мс	Интервал в миллисекундах, с которым коннектор перечитывает файлы в директории. Значение по умолчанию: `0` – коннектор перечитывает файлы в директории каждые 700 миллисекунд. Вам нужно выбрать в раскрывающемся списке **Режим опроса файла/папки** режим, в котором коннектор перечитывает файлы в директории. Введенное значение не должно быть меньше значения, которое вы ввели на вкладке **Основные параметры** в поле **Время ожидания изменений, сек**. Мы рекомендуем ввести значение меньше, чем значение, которое вы ввели в поле **TTL буфера событий**, так как это может негативно сказаться на работе функции Auditd.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
TTL буфера событий	Время жизни буфера для строк событий auditd в миллисекундах. Строки событий auditd попадают в коллектор Kaspersky SIEM Cloud и накапливаются в буфере. Это позволяет сгруппировать несколько строк событий auditd в одно событие auditd. Отсчет времени жизни буфера начинается при получении первой строки события auditd или при истечении предыдущего времени жизни буфера. Доступные значения: от 700 до 30 000. Значение по умолчанию: `2000`. Это поле доступно, если вы включили переключатель **Auditd** на вкладке **Основные параметры**. Строки событий auditd, накопленные в буфере, хранятся в оперативной памяти сервера. Мы рекомендуем с осторожностью увеличивать размер буфера, так как это может привести к использованию слишком большого количества оперативной памяти сервера коллектором Kaspersky SIEM Cloud. Вы можете просмотреть в метриках Kaspersky SIEM Cloud, сколько оперативной памяти сервера использует коллектор Kaspersky SIEM Cloud. Если вы хотите, чтобы время жизни буфера составляло более 30 000 миллисекунд, мы рекомендуем использовать другой транспорт доставки событий auditd. Например, вы можете использовать агента или предварительно накапливать события auditd в файле, после чего обрабатывать файл коллектором Kaspersky SIEM Cloud.
Заголовок транспорта	Регулярное выражение для событий auditd, по которому определяются строки событий auditd. Вы можете использовать значение по умолчанию или изменить его. Регулярное выражение должно содержать группы `record_type_name`, `record_type_value` и `event_sequence_number`. Если многострочное событие auditd содержит префикс, для первой строки события auditd префикс сохраняется, а для последующих – отбрасывается. Вы можете вернуться регулярному выражению для событий auditd по умолчанию, нажав на кнопку **Установить значение по умолчанию**.

Коннектор, тип 1c-log

Коннекторы с типом **1c-log** используются для получения данных из технологических журналов программы 1С при работе с агентами Linux. В качестве разделителя строк используется `\n`. Из многострочной записи о событии коннектор принимает только первую строку.

Доступные параметры коннектора с типом **1c-log** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **1c-log**. Обязательный параметр.

Параметр	Описание
Теги	Теги для поиска ресурса. Необязательный параметр.
Путь к директории	Полный путь к директории с файлами, с которыми требуется выполнять взаимодействие, например `/var/log/1c/logs/`. **Ограничения при использовании префиксов к путям файлов** Префиксы, которые невозможно использовать при указании путей к файлам: • `/*` • `/bin` • `/boot` • `/dev` • `/etc` • `/home` • `/lib` • `/lib64` • `/proc` • `/root` • `/run` • `/sys` • `/tmp` • `/usr/*` • `/usr/bin/` • `/usr/local/*` • `/usr/local/sbin/` • `/usr/local/bin/` • `/usr/sbin/` • `/usr/lib/` • `/usr/lib64/` • `/var/*` • `/var/lib/` • `/var/run/` • `/opt/kaspersky/kuma/` Приведенные префиксы используются системой в качестве регулярных выражений для проверки пути. Символ * в префиксах соответствует любой последовательности символов и не должен указываться в самом пути вручную, если это не часть допустимого пути. Файлы по указанным ниже путям доступны: • `/opt/kaspersky/kuma/clickhouse/logs/` • `/opt/kaspersky/kuma/metrics/log/` Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

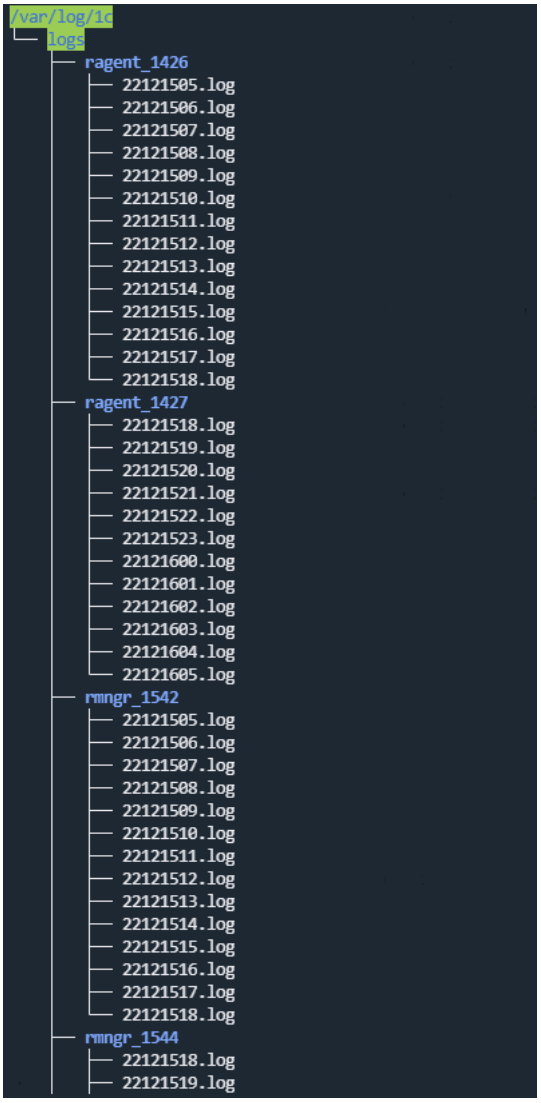
Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Режим опроса файла/папки	Режим, в котором коннектор перечитывает файлы в директории: • **Отслеживать изменения** – коннектор перечитывает файлы в директории с интервалом в миллисекундах, указанным в поле **Интервал запросов, мс**, если файлы не обновляются. Значение по умолчанию. Например, если файлы постоянно обновляются, а в поле **Интервал запросов, мс** вы ввели `5000`, коннектор будет перечитывать файлы постоянно, а не с интервалом в 5000 миллисекунд. Если файлы не обновляются, коннектор будет перечитывать их с интервалом в 5000 миллисекунд. • **Отслеживать периодически** – коннектор перечитывает файлы в директории с интервалом в миллисекундах, указанным в поле **Интервал запросов, мс**, вне зависимости от того, обновляются файлы или нет.
Интервал запросов, мс.	Интервал в миллисекундах, с которым коннектор перечитывает файлы в директории. Значение по умолчанию: `0` – коннектор перечитывает файлы в директории каждые 700 миллисекунд. Вам нужно выбрать в раскрывающемся списке **Режим опроса файла/папки** режим, в котором коннектор перечитывает файлы в директории.
Кодировка символов	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.

Схема работы коннектора:

1. Происходит поиск всех файлов технологических журналов 1С. Требования к файлам журналов:

   - Файлы с расширением LOG создаются в директории журналов (по умолчанию `/var/log/1c/logs/`) в поддиректории каждого процесса (см. рисунок по ссылке ниже).

Пример поддерживаемой структуры технологических журналов 1c



Пример поддерживаемой структуры технологических журналов 1c

- События записываются в файл в течение часа, после чего создается следующий файл журнала.
- Название файлов имеет следующий формат: <ГГ><ММ><ДД><ЧЧ>.log. Например, 22111418.log – файл, созданный в 2022 году, в 11 месяце, 14 числа в 18 часов.
- Каждое событие начинается с времени события в формате <мм>:<сс>.<микросекунды>-<длительность в микросекундах>.

2. Отбрасываются уже обработанные файлы. Сведения об обработанных файлах хранятся в файле /<рабочая директория коллектора>/1c_log_connector/state.json.

3. Принимаются на обработку новые события, при этом время события приводится к формату RFC3339.

4. Обрабатывается следующий в очереди файл.

Ограничения коннектора:

- Установка коллектора с коннектором 1c-log на ОС Windows не поддерживается. Для обеспечения передачи файлов с журналами 1С для обработки коллектором KUMA выполните следующие действия:

  1. На сервере Windows предоставьте доступ для чтения по сети к папке с журналами 1С.
  2. На сервере Linux примонтируйте сетевую папку с журналами 1С на сервере Linux (см. список поддерживаемых ОС).
  3. На сервере Linux установите коллектор, который будет обрабатывать файлы с журналами 1С из примонтированной сетевой папки.

- Из многострочной записи о событии на обработку принимается только первая строка.
- Нормализатор обрабатывает только следующие типы событий:
  - ADMIN.
  - ATTN.
  - CALL.
  - CLSTR.
  - CONN.
  - DBMSSQL.
  - DBMSSQLCONN.
  - DBV8DBENG.
  - EXCP.
  - EXCPCNTX.
  - HASP.
  - LEAKS.
  - LIC.
  - MEM.
  - PROC.
  - SCALL.
  - SCOM.
  - SDBL.
  - SESN.

- SINTEG.
- SRVC.
- TLOCK.
- TTIMEOUT.
- VRSREQUEST.
- VRSRESPONSE.

Коннектор, тип 1c-xml

Коннекторы с типом **1c-xml** используются для получения данных из журналов регистрации программы 1С при работе с агентами Linux. При обработке коннектором многострочные события преобразовываются в однострочные.

Доступные параметры коннектора с типом **1c-xml** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **1c-xml**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.

Параметр	Описание
Путь к директории	Полный путь к директории с файлами, с которыми требуется выполнять взаимодействие, например `/var/log/1c/logs/`. **Ограничения при использовании префиксов к путям файлов** Префиксы, которые невозможно использовать при указании путей к файлам: • `/*` • `/bin` • `/boot` • `/dev` • `/etc` • `/home` • `/lib` • `/lib64` • `/proc` • `/root` • `/run` • `/sys` • `/tmp` • `/usr/*` • `/usr/bin/` • `/usr/local/*` • `/usr/local/sbin/` • `/usr/local/bin/` • `/usr/sbin/` • `/usr/lib/` • `/usr/lib64/` • `/var/*` • `/var/lib/` • `/var/run/` • `/opt/kaspersky/kuma/` Приведенные префиксы используются системой в качестве регулярных выражений для проверки пути. Символ * в префиксах соответствует любой последовательности символов и не должен указываться в самом пути вручную, если это не часть допустимого пути. Файлы по указанным ниже путям доступны: • `/opt/kaspersky/kuma/clickhouse/logs/` • `/opt/kaspersky/kuma/metrics/log/` Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Режим опроса файла/папки	Режим, в котором коннектор перечитывает файлы в директории: • **Отслеживать изменения** – коннектор перечитывает файлы в директории с интервалом в миллисекундах, указанным в поле **Интервал запросов, мс**, если файлы не обновляются. Значение по умолчанию. Например, если файлы постоянно обновляются, а в поле **Интервал запросов, мс** вы ввели `5000`, коннектор будет перечитывать файлы постоянно, а не с интервалом в 5000 миллисекунд. Если файлы не обновляются, коннектор будет перечитывать их с интервалом в 5000 миллисекунд. • **Отслеживать периодически** – коннектор перечитывает файлы в директории с интервалом в миллисекундах, указанным в поле **Интервал запросов, мс**, вне зависимости от того, обновляются файлы или нет.
Интервал запросов, мс	Интервал в миллисекундах, с которым коннектор перечитывает файлы в директории. Значение по умолчанию: `0` – коннектор перечитывает файлы в директории каждые 700 миллисекунд. Вам нужно выбрать в раскрывающемся списке **Режим опроса файла/папки** режим, в котором коннектор перечитывает файлы в директории.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Схема работы коннектора:

1. Происходит поиск всех файлов с журналами 1С с расширением XML внутри указанной директории. Журналы помещаются в директорию или вручную, или через приложение, написанное на языке 1С, например с помощью функции `ВыгрузитьЖурналРегистрации()`. Коннектор поддерживает журналы, полученные только таким образом. Подробнее о том, как получить журналы 1С, см. в официальной документации 1С.

2. Файлы сортируются по возрастанию времени последнего изменения. Коннектор сохраняет сведения о последнем обработанном файле и не обрабатывает файлы, измененные раньше него. При сбросе состояния (например, при обнаружении пустого файла) ранее обработанные файлы могут быть обработаны повторно.

   Сведения об обработанных файлах хранятся в файле `/<рабочая директория коллектора>/1c_xml_connector/state.ini` и имеют следующий формат: `offset=<число>\ndev=<число>\ninode=<число>`.

3. В каждом непрочитанном файле определяются события.

4. События из файла по очереди принимаются на обработку, при этом многострочные события преобразовываются в однострочные события.

Ограничения коннектора:

- Установка коллектора с коннектором 1c-xml на устройствах под управлением Windows не поддерживается. Для обеспечения передачи файлов с журналами 1С для обработки коллектором Kaspersky SIEM Cloud выполните следующие действия:

  1. На сервере Windows предоставьте доступ для чтения по сети к папке с журналами 1С.

  2. На сервере Linux примонтируйте сетевую папку с журналами 1С на сервере Linux (см. список поддерживаемых ОС).

  3. На сервере Linux установите коллектор, который будет обрабатывать файлы с журналами 1С из примонтированной сетевой папки.

- Не читаются файлы с неправильным форматом событий. Например, если теги события в файле на русском языке, коллектор не прочитает такие события.

  Пример правильного XML-файла с событием

```
<?xml version="1.0" encoding="UTF-8"?>
<v8e:EventLog xmlns: v8e="http://v8.1c.ru/eventLog"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <v8e:Event>
                <v8e:Level>Information</v8e:Level>
                <v8e:Date>2022-12-07T01:55:44+03:00</v8e:Date>
                <v8eApplicationName>generator.go</v8e:ApplicationName>

<v8e:ApplicationPresentation>generator.go</v8e:ApplicationPresentation>
                <v8e:Event>Test event type: Count test</v8e:Event>
                <v8e:EventPresentation></v8e:Event Presentation>
                <v8e:User>abcd_1234</v8e:User>
                <v8e:UserName>TestUser</v8e:UserName>
                <v8e:Computer>Test OC</v8e:Computer>
                <v8e:Metadata></v8e:Metadata>
                <v8e:MetadataPresentation></v8e:MetadataPresentation>
                <v8e:Comment></v8e:Comment>
                <v8e:Data>
                        <v8e:Name></v8e:Name>
                        <v8e:CurrentOSUser></v8e:CurrentOSUser>
                </v8e:Data>
                <v8e:DataPresentation></v8e:DataPresentation>
                <v8e:TransactionStatus>NotApplicable</v8e:TransactionStatus>
                <v8e:TransactionID></v8e:TransactionID>
                <v8e:Connection>0</v8e:Connection>
                <v8e:Session></v8e:Session>
                <v8e:ServerName>kuma-test</v8e:ServerName>
                <v8e:Port>80</v8e:Port>
                <v8e:SyncPort>0</v8e:SyncPort>
        </v8e:Event>
</v8e:EventLog>
```

  Пример обработанного события

```
<v8e:Event><v8e:Level>Information</v8e:Level><v8e:Date>2022-12-
07T01:55:44+03:00</v8e:Date><v8e:ApplicationName>generator.go</v8e:ApplicationName><v8e:ApplicationPresentation>generator.go
</v8e:ApplicationPresentation><v8e:Event>Test event type: Count
test</v8e:Event><v8e:EventPresentation></v8e:EventPresentation><v8e:User>abcd_1234</v8e:User><v8e:UserName>TestUser</v8e:Use
rName><v8e:Computer>Test
OC</v8e:Computer><v8e:Metadata></v8e:Metadata><v8e:MetadataPresentation></v8e:MetadataPresentation><v8e:Comment></v8e:Commen
t><v8e:Data><v8e:Name></v8e:Name><v8e:CurrentOSUser></v8e:CurrentOSUser></v8e:Data><v8e:DataPresentation></v8e:DataPresentat
ion><v8e:TransactionStatus>NotApplicable</v8e:TransactionStatus><v8e:TransactionID></v8e:TransactionID><v8e:Connection>0</v8
e:Connection><v8e:Session></v8e:Session><v8e:ServerName>kuma-
test</v8e:ServerName><v8e:Port>80</v8e:Port><v8e:SyncPort>0</v8e:SyncPort></v8e:Event>
```

Пример обработанного события

- При наличии в директории пустого файла журнала (файла без событий) коннектор сбрасывает сведения о последнем обработанном файле. В результате ранее обработанные файлы могут быть обработаны повторно. Чтобы избежать повторной обработки событий, используйте один из следующих способов:

  - Используйте маску имени файла, исключающую новые пустые файлы из обработки, и переименуйте файл после записи первого события.

  - Перед созданием нового файла переименуйте уже обработанные файлы так, чтобы они перестали соответствовать маске поиска коннектора.

- Если дополнить уже прочитанный коннектором файл новыми событиями и если этот файл не является последним прочитанным файлом в директории, все события из файла будут обработаны заново.

Коннектор, тип diode

Коннекторы с типом **diode** используются для однонаправленной передачи данных в промышленных ICS-сетях с помощью диода данных. Доступные параметры коннектора с типом **diode** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **diode**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.

Параметр	Описание
Директория с событиями от диода данных	Полный путь к директории на сервере коллектора Kaspersky SIEM Cloud, в которую диод данных перемещает файлы с событиями из изолированного сегмента сети. После считывания коннектором файлы удаляются из директории. Максимальная длина пути: до 255 символов в кодировке Unicode. **Ограничения при использовании префиксов к путям** Префиксы, которые невозможно использовать при указании путей к файлам: • `/*` • `/bin` • `/boot` • `/dev` • `/etc` • `/home` • `/lib` • `/lib64` • `/proc` • `/root` • `/run` • `/sys` • `/tmp` • `/usr/*` • `/usr/bin/` • `/usr/local/*` • `/usr/local/sbin/` • `/usr/local/bin/` • `/usr/sbin/` • `/usr/lib/` • `/usr/lib64/` • `/var/*` • `/var/lib/` • `/var/run/` • `/opt/kaspersky/kuma/` Приведенные префиксы используются системой в качестве регулярных выражений для проверки пути. Символ * в префиксах соответствует любой последовательности символов и не должен указываться в самом пути вручную, если это не часть допустимого пути. Файлы по указанным ниже путям доступны: • `/opt/kaspersky/kuma/clickhouse/logs/` • `/opt/kaspersky/kuma/metrics/log/` Обязательный параметр.

Параметр	Описание
Разделитель	Символ, определяющий границу между событиями: • **\n**; • **\t**; • **\0**. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений. Вам нужно выбрать одинаковое значение в раскрывающемся списке **Разделитель** в параметрах коннектора и точки назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Количество обработчиков	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Интервал запросов, сек.	Интервал в секундах для считывания файлов из директории с событиями от диода данных. Значение по умолчанию: 2 секунды.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
Сжатие	Определяет метод распаковки данных, поступающих в коннектор. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**. Вам нужно выбрать одинаковое значение в раскрывающемся списке **Snappy** в параметрах коннектора и точки назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.

Коннектор, тип ftp

Коннекторы с типом **ftp** используются для получения данных по протоколу File Transfer Protocol при работе с агентами Windows и Linux. Доступные параметры коннектора с типом **ftp** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **ftp**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.

Параметр	Описание

URL	URL-адрес файла или маски файлов, начинающийся со схемы `'ftp://'`. Для маски файлов вы можете использовать символы `* ? [...]`.
	Шаблоны масок для файлов
	Маски:
	• `'*'` – соответствует любой последовательности символов;
	• `'[' [ '^' ] { < диапазон символов > } ']'` – класс символов (не должен быть пустым);
	• `'?'` – соответствует любому одиночному символу.
	Диапазоны символов:
	• `[0-9]` – числа;
	• `[a-zA-Z]` – буквы латинского алфавита.
	Пример:
	Маски можно использовать как в путях Linux, так и Windows с заменой прямой косой черты на обратную:
	• Для Linux:
	  • `/var/log/*som?[1-9].log`
	  • `/mnt/dns_logs/*/dns.log`
	  • `/mnt/proxy/access*.log`
	• Для Windows:
	  • `C:\var\log\test123.log`
	  • `D:\data\*\report?.txt`
	Если URL-адрес не содержит номер порта FTP-сервера, автоматически указывается номер порта `21`.
	Обязательный параметр.

Секрет	
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Коннектор, тип sftp

Коннекторы с типом **sftp** используются для получения данных по протоколу Secure File Transfer Protocol при работе с агентами Windows и Linux.

Коннектор sftp получает события из файлов на удаленном SFTP-сервере. Коннектор периодически просматривает указанные файлы по имени или маске и передает в нормализатор новые данные. Для работы коннектор требует SSH-соединения с SFTP-сервером.

Коннектор рассчитан на файлы журналов, строки в которые добавляются в конец файла. При очистке файла, уменьшении его размера или изменении файла без изменения его размера коннектор перечитает весь файл с начала и передаст события в нормализатор повторно.

Интервал опроса директории и чтения файлов: 2 секунды

Размер буфера: 1 МБ

Доступные параметры коннектора с типом **sftp** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **sftp**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.

URL	URL-адрес файла журнала или маски файлов, начинающийся со схемы `'sftp://'`, например `sftp://example.com:22/path/to/file.log`. Для маски файлов вы можете использовать символы `* ? [...]`. Использование масок в именах директорий не допускается.
	Kaspersky SIEM Cloud получает информацию только из файлов, хранящихся в последней директории, указанной в пути. Например, вы указываете следующий путь:
	`sftp://<host_name>:<port>/<directory_name1>/<directory_name2>/<mask>`
	В таком случае Kaspersky SIEM Cloud получит информацию только из файлов из директории 2. Если в директории 2 хранятся вложенные директории, файлы из них прочитаны не будут.
	Шаблоны масок для файлов
	Маски:
	• `'*'` – соответствует любой последовательности символов;
	• `'[' [ '^' ] { < диапазон символов > } ']'` – класс символов (не должен быть пустым);
	• `'?'` – соответствует любому одиночному символу.
	Диапазоны символов:
	• `[0-9]` – числа;
	• `[a-zA-Z]` – буквы латинского алфавита.
	Пример:
	Маски можно использовать в именах файлов как в путях Linux, так и Windows с заменой прямой косой черты на обратную:
	• Для Linux:
	  • `/var/log/*som?[1-9].log`
	  • `/mnt/proxy/access*.log`
	• Для Windows:
	  • `C:\var\log\test123.log`
	  • `D:\data\log\report?.txt`
	Если URL-адрес не содержит номер порта SFTP-сервера, автоматически указывается номер порта `22`.
	Обязательный параметр.

Открытые ключи SSH-сервера	Открытые ключи, используемые для проверки подлинности SFTP-сервера при установке SSH-соединения. Вы можете указать несколько ключей разных типов, коннектор автоматически выберет подходящий ключ.
	Формат: `<key_type><base64 value>`
	Пример ключа: ssh-ed25519 ABCD...
	На сервере открытые ключи лежат по следующему пути:
	`/etc/ssh/ssh_host_*_key.pub`
	Вы также можете получить открытые ключи, выполнив команду:
	`ssh-keyscan [-p port] [-t type] [host | addrlist namelist]`
	Примеры команд:
	`ssh-keyscan example.com`
	`ssh-keyscan -p 2222 -t rsa,ed25519 example.com`
	Обязательный параметр.

Параметр	Описание
Секрет	Секрет, в котором хранятся учетные данные для подключения к SFTP-серверу. Поддерживаются секреты с типом **credentials** и **ssh private key**. Секрет должен содержать либо имя пользователя и пароль, либо имя пользователя и закрытый SSH-ключ. Если для подключения к SFTP-серверу учетные данные не требуются, при заполнении имени пользователя и пароля оставьте поля пустыми. Вы можете выбрать существующий секрет или создать новый секрет. Для создания секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать секрет?** *Чтобы создать секрет:* 1. В поле **Название** введите название секрета. 2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору. 3. При необходимости в поле **Описание** введите описание секрета. 4. Нажмите на кнопку **Создать**. Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка файлов, полученных с SFTP-сервера. По умолчанию используется кодировка UTF-8. Необязательный параметр.

Коннектор, тип nfs

Коннекторы с типом **nfs** используются для получения данных по протоколу Network File System при работе с агентами Windows и Linux. Доступные параметры коннектора с типом **nfs** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **nfs**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	Путь до удаленной директории в формате `nfs://<host name>/<path>`. Обязательный параметр.
Маска имени файла	Маска, по которой фильтруются файлы с событиями. Допустимо использование масок "`*`", "`?`", "`[...]`".
Интервал запросов, сек.	Интервал опроса в секундах. Промежуток времени, через который перечитываются файлы с удаленной системы. Значение по умолчанию: `0`.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Коннектор, тип wmi

Коннекторы с типом **wmi** используются для получения данных с помощью Windows Management Instrumentation при работе с агентами Windows. Доступные параметры коннектора с типом **wmi** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **wmi**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.
URL	URL-адрес коллектора, который вы создали для получения данных с помощью Windows Management Instrumentation, например `kuma-collector.example.com:7221`. При создании коллектора автоматически создается агент, который будет получать данные на удаленном устройстве и перенаправлять их в сервис коллектора. Если вы знаете, на каком сервере будет установлен сервис коллектора, URL-адрес известен заранее. Вы можете ввести URL-адрес коллектора в поле **URL** после завершения мастера установки. Для этого вам нужно предварительно скопировать URL-адрес коллектора в разделе **Ресурсы** → **Активные сервисы**. Обязательный параметр.
Учетные данные по умолчанию	Вам нужно указать учетные данные для подключения к хостам, которые можно использовать по умолчанию в таблице **Удаленные хосты**. Поле является обязательным, если в таблице **Удаленные хосты** не указан секрет хотя бы для одного хоста.

Параметр	Описание
Удаленные хосты	Параметры удаленных Windows-устройств, к которым требуется установить подключение: • **Сервер** – IP-адрес или имя устройства, с которого необходимо принимать данные, например `machine-1`. Не допускается использование символов кириллицы. Обязательный параметр. • **Домен** – название домена, в котором расположено удаленное устройство, например, `example.com`. Не допускается использование символов кириллицы. Обязательный параметр. • **Тип журналов** – название журналов Windows, которые требуется получить. По умолчанию в этом раскрывающемся списке отображаются только предварительно настроенные журналы, но вы можете расширить список пользовательскими журналами. Для этого введите название пользовательских журналов в поле **Журналы Windows**, после чего нажмите на клавишу **ENTER**. Конфигурация сервисов и ресурсов Kaspersky SIEM Cloud может потребовать дополнительных изменений для правильной обработки настраиваемых журналов. Журналы, доступные по умолчанию: • Application. • ForwardedEvents. • Security. • System. • HardwareEvents. Если в одном из подключений WMI используется хотя бы один журнал с неверным названием, агент, использующий коннектор, не будет получать события из всех журналов данного подключения, даже если названия остальных журналов указаны верно. При этом подключения WMI-агента, в которых все названия журналов указаны правильно, будет работать правильно. Обязательный параметр. • **Секрет** – учетные данные для доступа к удаленному Windows-устройству с правами на чтение журналов. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите **Создать**. При создании секрета в поле **Пользователь** не требуется указывать домен для доступа к хосту, поскольку используется значение, указанное в поле **Домен** в таблице **Удаленные хосты**. Если вы хотите изменить параметры существующего секрета, нажмите на значок карандаша ✎. Если оставить в этом поле значение **по умолчанию**, для подключения к удаленным Windows-устройствам будут использоваться учетные данные, указанные в поле **Учетные данные, используемые по умолчанию**. **Как создать секрет?** *Чтобы создать секрет:* 1. В поле **Название** введите название секрета. 2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору. 3. При необходимости в поле **Описание** введите описание секрета. 4. Нажмите на кнопку **Создать**. Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**. Вы можете добавить несколько удаленных Windows-устройств или удалить удаленное Windows-устройство. Для добавления удаленного Windows-устройства нажмите на кнопку **+ Добавить**. Для удаления удаленного Windows-устройства установите рядом с ним флажок и нажмите на кнопку **Удалить**. Также с помощью кнопки **Импортировать** вы можете импортировать файл со списком удаленных Windows-устройств в формате TSV, чтобы не заполнять поля вручную, когда таких устройств много. Kaspersky SIEM Cloud автоматически подставит данные из файла и выполнит проверку. Для некорректно заполненных полей отобразится ошибка. Вы можете внести правки для таких полей вручную и сохранить параметры.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Параметр	Описание
Режим TLS	Режим шифрования TLS. При использовании шифрования TLS вы не можете указать IP-адрес в поле **URL** на вкладке **Основные параметры**. Доступные значения: • **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию. • **Включено** – использовать шифрование TLS, но без верификации сертификатов.
Сжатие	Определяет метод распаковки данных, поступающих в коннектор. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.

При изменении коннектора этого типа параметры **Режим TLS** и **Сжатие** видны и доступны как на коннекторе-ресурсе, так и на коллекторе. Если вы используете коннектор этого типа на коллекторе, значения параметров **Режим TLS** и **Сжатие** передаются в точку назначения автоматически созданных агентов.

Получение событий с удаленного устройства

Условия для получения событий с удаленного устройства Windows с агентом Kaspersky SIEM Cloud:

- Для запуска агента Kaspersky SIEM Cloud на удаленном устройстве вам нужно использовать учетную запись с правами Log on as a service.
- Для получения событий от агента Kaspersky SIEM Cloud вам нужно использовать учетную запись с правами Event Log Readers. Для серверов домена может быть создана одна такая учетная запись, чтобы через групповую политику ее права на чтение логов можно было распространить на все серверы и рабочие станции домена.
- На удаленных устройствах Windows необходимо открыть следующие TCP-порты 135, 445, 49152-65535.
- На удаленных устройствах требуется запустить следующие службы:
  - Remote Procedure Call (RPC)
  - RPC Endpoint Mapper

Коннектор, тип wec

Коннекторы с типом **wec** используются для получения данных с помощью Windows Event Forwarding (WEF) и Windows Event Collector (WEC) или локальных журналов ОС хоста под управлением Windows при работе с агентами Windows. Доступные параметры коннектора с типом **wec** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **wec**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.

Параметр	Описание
URL	URL-адрес коллектора, который вы создали для получения данных с помощью Windows Event Collector, например `kuma-collector.example.com:7221`. При создании коллектора автоматически создается агент, который будет получать данные на удаленном устройстве и перенаправлять их в сервис коллектора. Если вы знаете, на каком сервере будет установлен сервис коллектора, URL-адрес известен заранее. Вы можете ввести URL-адрес коллектора в поле **URL** после завершения мастера установки. Для этого вам нужно предварительно скопировать URL-адрес коллектора в разделе **Ресурсы** → **Активные сервисы**. Обязательный параметр.
Журналы Windows	Названия журналов Windows, которые требуется получить. По умолчанию в этом раскрывающемся списке отображаются только предварительно настроенные журналы, но вы можете расширить список пользовательскими журналами. Для этого введите название пользовательских журналов в поле **Журналы Windows**, после чего нажмите на клавишу **ENTER**. Конфигурация сервисов и ресурсов Kaspersky SIEM Cloud может потребовать дополнительных изменений для правильной обработки настраиваемых журналов. Преднастроенные журналы: • Application. • ForwardedEvents. • Security. • System. • HardwareEvents. Если неверно указать название хотя бы одного журнала, в этом случае агент, использующий коннектор, не будет получать события из всех журналов, даже если названия остальных журналов указаны верно. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
Режим TLS	Режим шифрования TLS. При использовании шифрования TLS вы не можете указать IP-адрес в поле **URL** на вкладке **Основные параметры**. Доступные значения: • **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию. • **Включено** – использовать шифрование TLS, но без верификации сертификатов.
Сжатие	Определяет метод распаковки данных, поступающих в коннектор. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.

При изменении коннектора этого типа параметры **Режим TLS** и **Сжатие** видны и доступны как на коннекторе-ресурсе, так и на коллекторе. Если вы используете коннектор этого типа на коллекторе, значения параметров **Режим TLS** и **Сжатие** передаются в точку назначения автоматически созданных агентов.

Для запуска агента KUMA на удаленном устройстве вам нужно использовать сервисную учетную запись с правами Log on as a service. Для получения событий из журнала ОС сервисная учетная запись также должна обладать правами Event Log Readers.

Вы можете создать одну учетную запись с правами Log on as a service и Event Log Readers, а затем права этой учетной записи на чтение журналов распространить на все серверы и рабочие станции домена с помощью групповой политики.

Мы рекомендуем запретить для сервисной учетной записи возможность интерактивного входа.

Коннектор, тип etw

Коннекторы с типом **etw** используются для получения расширенных журналов DNS-серверов. Доступные параметры коннектора с типом **etw** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **etw**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	URL-адрес DNS-сервера. Обязательный параметр.
Имя сессии	Имя сессии, которое соответствует ETW-провайдеру Microsoft-Windows-DNSServer {EB79061A-A566-4698-9119-3ED2807060E7}. Если в коннекторе с типом **etw** имя сессии указано неправильно, указан неправильный провайдер в сессии или указан неправильный режим отправки событий (для правильной отправки событий на стороне Windows Server должен быть указан режим Real time или File and Real time), от агента не будут поступать события, в журнале агента на Windows будет зарегистрирована ошибка, а статус агента будет зеленым. При этом попытки получить события каждые 60 сек не будет. Если вы изменяете параметры сессии на стороне Windows, вам нужно перезапустить агент etw и/или сессию, чтобы изменения были применены. Подробнее о настройке параметров сессии на стороне Windows для получения событий DNS-сервера, см. в разделе Настройка получения событий DNS-сервера с помощью агента ETW. Обязательный параметр.
Извлекать информацию о событии	Переключатель, включающий извлечение минимального количества данных о событии, которое возможно без необходимости скачивать сторонние метаданные с диска. Такой способ позволяет сэкономить CPU на машине с агентом. По умолчанию этот переключатель включен и извлекаются все данные о событии.
Извлекать свойства события	Переключатель, включающий извлечение свойств событий. Если этот переключатель выключен, свойства события не будут извлечены и это позволит сэкономить CPU на машине с агентом. По умолчанию этот переключатель включен и свойства события извлекаются. Вы можете включить переключатель **Извлекать свойства события**, только если включен переключатель **Извлекать информацию о событии**.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
Режим TLS	Режим шифрования TLS. При использовании шифрования TLS вы не можете указать IP-адрес в поле **URL** на вкладке **Основные параметры**. Доступные значения: • **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию. • **Включено** – использовать шифрование TLS, но без верификации сертификатов.

Параметр	Описание
Сжатие	Определяет метод распаковки данных, поступающих в коннектор. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.

При изменении коннектора этого типа параметры **Режим TLS** и **Сжатие** видны и доступны как на коннекторе-ресурсе, так и на коллекторе. Если вы используете коннектор этого типа на коллекторе, значения параметров **Режим TLS** и **Сжатие** передаются в точку назначения автоматически созданных агентов.

Коннектор, тип snmp

Коннекторы с типом **snmp** используются для получения данных с помощью Simple Network Management Protocol при работе с агентами Windows и Linux. Для обработки событий, полученных по протоколу SNMP, вам нужно использовать нормализатор с типом json. Поддерживаемые версии протокола SNMP:

- snmpV1.
- snmpV2.
- snmpV3.

В агенте можно использовать только один коннектор **snmp**, созданный в параметрах агента. При необходимости использования нескольких коннекторов **snmp**, один или все коннекторы **snmp** нужно создать как отдельный ресурс и выбрать в параметрах подключения.

Доступные параметры коннектора с типом **snmp** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **snmp**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Параметр	Описание

SNMP-ресурс	Параметры подключения к SNMP-ресурсу:
	• **Версия SNMP** – версия используемого протокола SNMP.
	Обязательный параметр.
	• **Хост** – имя или IP-адрес хоста. Доступные форматы:
	  • `<host name>`;
	  • `<IPv4 address>`;
	  • `<IPv6 address>`.
	Обязательный параметр.
	• **Порт** – Номер порта для подключения к хосту. Как правило используется значение `161` или `162`.
	Обязательный параметр.
	• **Секрет** – секрет, в котором хранятся учетные данные для подключения через Simple Network Management Protocol. Тип секрета должен соответствовать версии SNMP.
	Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша ✎.
	Как создать секрет?
	Чтобы создать секрет:
	1. В поле **Название** введите название секрета.
	2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору.
	3. При необходимости в поле **Описание** введите описание секрета.
	4. Нажмите на кнопку **Создать**.
	Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**.
	Обязательный параметр.
	Вы можете добавить несколько подключений к SNMP-ресурсам или удалить подключение к SNMP-ресурсу. Для добавления подключения к SNMP-ресурсу нажмите на кнопку **+ SNMP-ресурс**. Для удаления подключения к SNMP-ресурсу нажмите рядом с ним на значок удаления ✕.

Параметры	Правила именования получаемых данных, по которым идентификаторы объектов OID будут преобразовываться в ключи, с которыми сможет взаимодействовать нормализатор. Доступные параметры: • **Название параметра** – название для типа данных, например `Имя узла` или `Время работы узла`. Обязательный параметр. • **OID** – уникальный идентификатор, который определяет, где искать требуемые данные на источнике событий, например `1.3.6.1.2.1.1.5`. Kaspersky SIEM Cloud запрашивает данные с помощью команды SNMP GET. Обязательный параметр. • **Ключ** – уникальный идентификатор, который возвращается в ответ на запрос к устройству со значением запрошенного параметра, например `sysName`. Вы можете обращаться к ключу при нормализации данных. Обязательный параметр. • **MAC-адрес** – если этот флажок установлен, Kaspersky SIEM Cloud правильно производит декодирование данных, где OID содержит данные о MAC-адресе в формате OctetString. После декодирования MAC-адрес будет преобразован в формат `Строка` вида XX:XX:XX:XX:XX:XX. Вы можете выполнить следующие действия с правилами: • Добавить несколько правил. Для добавления правила нажмите на кнопку **+ Добавить**. • Удалить правила. Для удаления правила установите рядом с ним флажок и нажмите на кнопку **Удалить**. • Очистить параметры правил. Для этого нажмите на кнопку **Очистить значения**.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Коннектор, тип snmp-trap

Коннекторы с типом **snmp-trap** используются для пассивного приема событий с помощью ловушек SNMP (англ. SNMP traps) при работе с агентами Windows и Linux. В коннекторе события snmp-trap принимаются и подготавливаются к нормализации путем сопоставления идентификаторов SNMP-объектов с временными ключами. Затем сообщение необходимо передать в JSON-нормализатор, где временные ключи будут сопоставлены с полями Kaspersky SIEM Cloud и будет создано событие. Для обработки событий, полученных по SNMP, вам нужно использовать нормализатор с типом json. Поддерживаемые версии протокола SNMP:

- snmpV1.
- snmpV2.

Доступные параметры коннектора с типом **snmp-trap** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **snmp-trap**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

SNMP-ресурс	Параметры соединения для получения событий snmp-trap:
	• **Версия SNMP** – версия используемого протокола SNMP:
	  • **snmpV1**;
	  • **snmpV2**.
	  Например, Windows по умолчанию использует версию протокола SNMP snmpV2.
	  Обязательный параметр.
	• **URL** – URL-адрес для получения событий SNMP trap. Вы можете ввести URL-адрес в одном из следующих форматов:
	  • `<host name>:<port number>`;
	  • `<IPv4 address>:<port number>`;
	  • `<IPv6 address>:<port number>`;
	  • `:<port number>`.
	  Обязательный параметр.
	Вы можете добавить несколько соединений или удалить соединение. Для добавления соединения нажмите на кнопку **+ SNMP-ресурс**. Для удаления SNMP-ресурса нажмите рядом с ним на значок удаления ✕.

Параметр	Описание
Параметры	Правила именования получаемых данных, по которым идентификаторы объектов OID будут преобразовываться в ключи, с которыми сможет взаимодействовать нормализатор. Доступные параметры: • **Название параметра** – название для типа данных, например `Имя узла` или `Время работы узла`. Обязательный параметр. • **OID** – уникальный идентификатор, который определяет, где искать требуемые данные на источнике событий, например `1.3.6.1.2.1.1.5`. Kaspersky SIEM Cloud запрашивает данные с помощью команды SNMP GET. Обязательный параметр. • **Ключ** – уникальный идентификатор, который возвращается в ответ на запрос к устройству со значением запрошенного параметра, например `sysName`. Вы можете обращаться к ключу при нормализации данных. Обязательный параметр. • **MAC-адрес** – если этот флажок установлен, Kaspersky SIEM Cloud правильно производит декодирование данных, где OID содержит данные о MAC-адресе в формате OctetString. После декодирования MAC-адрес будет преобразован в формат `Строка` вида XX:XX:XX:XX:XX:XX. Вы можете выполнить следующие действия с правилами: • Добавить несколько правил. Для добавления правила нажмите на кнопку **+ Добавить**. • Удалить правила. Для удаления правила установите рядом с ним флажок и нажмите на кнопку **Удалить**. • Очистить параметры правил. Для этого нажмите на кнопку **Очистить значения**. • Заполнить таблицу сопоставлениями для значений OID, поступающих в журналах WinEventLog. Для этого нажмите на кнопку **Применить значения OID для WinEventLog**. Если в поступающих событиях необходимо определить и нормализовать больше данных, дополните таблицу строками с перечнем OID-объектов и их ключей. Данные обрабатываются по принципу списка разрешенных: объекты, которые не указаны в таблице, не будут переданы в нормализатор для дальнейшей обработки.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**. При получении событий snmp-trap из Windows с русской локализацией мы рекомендуем изменить кодировку символов в коннекторе с типом **snmp-trap** на Windows 1251, если в событии получены недопустимые символы.

Коннектор, тип kata/edr

Коннекторы с типом **kata/edr** используются для получения данных KEDR по API. Доступные параметры коннектора с типом **kata/edr** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **kata/edr**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Поддерживаются следующие форматы URL-адресов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address><port number>`. IPv6-адреса можно указать в формате `[<IPv6 address>%<interface>:<port number>`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Вы можете добавить несколько URL-адресов и удалить URL-адрес. Kaspersky SIEM Cloud не позволяет сохранить ресурс или сервис если в поле URL есть знак табуляции или пробел. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр.

Параметр	Описание
Секрет	Секрет, в котором хранятся учетные данные для подключения к серверу KATA/EDR. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать секрет?** *Чтобы создать секрет:* 1. В поле **Название** введите название секрета. 2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору. 3. При необходимости в поле **Описание** введите описание секрета. 4. Нажмите на кнопку **Создать**. Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**. Обязательный параметр.
Внешний ID	Идентификатор для внешних систем. KUMA автоматически генерирует идентификатор и указывает его в этом поле.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. Мы рекомендуем применять конвертацию, только если в полях нормализованного события отображаются недопустимые символы. По умолчанию значение не выбрано.
Максимальное количество событий	Максимальное количество событий в одном запросе. По умолчанию используется значение, указанное на сервере KATA/EDR.
Время ожидания получения событий	Время ожидания получения событий от сервера KATA/EDR в секундах. Значение по умолчанию: `0` – используется значение, указанное на сервере KATA/EDR.
Время ожидания ответа	Время ожидания ответа от сервера KATA/EDR в секундах. Значение по умолчанию: `0` – 1800 секунд.
Фильтр KEDRQL	Фильтр запросов к серверу KATA/EDR. Подробнее о языке запросов см. в Справке KEDR.

Коннектор, тип vmware

Коннекторы с типом **vmware** используются для получения данных VMware vCenter по API. Доступные параметры коннектора с типом **vmware** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **vmware**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	URL-адрес API VMware. Вам нужно указать имя хоста и номер порта в URL-адресе. Вы можете указать только один URL-адрес. Обязательный параметр.

Параметр	Описание
Учетные данные VMware	Секрет, где хранится логин и пароль для подключения к API VMware. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша . **Как создать секрет?** *Чтобы создать секрет:* 1. В поле **Название** введите название секрета. 2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору. 3. При необходимости в поле **Описание** введите описание секрета. 4. Нажмите на кнопку **Создать**. Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**. Обязательный параметр.
Время ожидания, сек	Время ожидания в секундах между запросом, который не вернул события, и новым запросом. Значение по умолчанию: 5 секунд. Если вы указываете `0`, используется значение по умолчанию.
Количество запрашиваемых событий	Количество запрашиваемых событий из API VMware за один запрос. Значение по умолчанию: `100`. Максимальное значение: `1000`.
Начальная временная метка	Дата и время, начиная с которого события будут считываться из API VMware. По умолчанию события считываются из API VMware с момента запуска коллектора. При запуске после остановки коллектора, считывание событий будет происходить с последней сохраненной даты.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Параметр	Описание

Режим TLS	Режим шифрования TLS. При использовании шифрования TLS вы не можете указать IP-адрес в поле **URL** на вкладке **Основные параметры**. Доступные значения:
	• **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию.
	• **Включено** – использовать шифрование TLS, но без верификации сертификатов.
	• **Нестандартный CA** – использовать шифрование TLS с верификацией сертификата, подписанного центром сертификации. При выборе этого значения в раскрывающемся списке **Нестандартный CA** укажите секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать сертификат, подписанный центром сертификации?
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра Kaspersky SIEM Cloud (в примерах команд ниже используется OpenSSL).
	Чтобы создать сертификат, подписанный центром сертификации:
	1. Создайте ключ, который будет использоваться центром сертификации, например:
	`openssl genrsa -out ca.key 2048`
	2. Создайте сертификат для созданного ключа, например:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<common name of the certification authority host>" -out ca.crt`
	3. Создайте приватный ключ и запрос на его подписание в центре сертификации, например:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<common host name of the Kaspersky SIEM Cloud server>" -out server.csr`
	4. Создайте сертификат, подписанный центром сертификации. Вам нужно включить в переменную `subjectAltName` доменные имена или IP-адреса сервера, для которого вы создаете сертификат, например:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Загрузите созданный сертификат `server.crt` в веб-интерфейсе Kaspersky SIEM Cloud в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	Для использования сертификатов Kaspersky SIEM Cloud на сторонних устройствах вам нужно изменить расширение файла сертификата с CERT на CRT. В противном случае вы можете получить ошибку `x509: certificate signed by unknown authority`.

Коннектор, тип elastic

Коннекторы с типом **elastic** используются для получения данных Elasticsearch. Поддерживается работа с Elasticsearch версии 7.0.0. Доступные параметры коннектора с типом **elastic** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **elastic**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.

Параметр	Описание
Соединение	Параметры подключения к серверу Elasticsearch: • **URL** – URL-адрес сервера Elasticsearch. Вы можете добавить несколько URL-адресов или удалить URL-адрес. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр. • **Индекс** – имя индекса в Elasticsearch. Обязательный параметр. • **Запрос** – запрос в Elasticsearch. Мы рекомендуем указывать в запросе параметр `size` для предотвращения проблем с производительностью Kaspersky SIEM Cloud и Elasticsearch, а также параметр `sort` для направления сортировки. Для параметра `sort` в запросе возможны значения: `asc`, `desc` или пользовательское направление сортировки по конкретным полям в соответствии с синтаксисом Elasticsearch. Для сортировки по конкретному полю рекомендуется также указывать параметр `"missing" : "_first"` рядом с параметром `"order"` для предотвращения ошибок в случаях, когда это поле отсутствует в каком-либо документе. Например, `"sort": { "DestinationDnsDomain.keyword": {"order": "desc", "missing" : "_first" } }`. Подробнее о сортировке см. в документации Elasticsearch. Пример запроса: `"query" : { "match_all" : {} }, "size" : 25, "sort": {"_doc" : "asc"}` Обязательный параметр. • **Учетные данные Elastic** – секрет, в котором хранятся учетные данные для подключения к серверу Elasticsearch. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша ✎. **Как создать секрет?** *Чтобы создать секрет:* 1. В поле **Название** введите название секрета. 2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору. 3. При необходимости в поле **Описание** введите описание секрета. 4. Нажмите на кнопку **Создать**. Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**. • **Elastic fingerprint** – секрет, в котором хранятся секреты типа fingerprint для подключения к серверу Elasticsearch и секреты типа certificate для использования CA сертификата. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша ✎. • **Интервал запросов, сек** – интервал выполнения между запросами к серверу Elasticsearch в секундах в случае, если в предыдущем запросе отсутствовали события. Если Elasticsearch содержал события в момент выполнения запроса, коннектор будет получать события до момента, пока не будут получены все доступные события из Elasticsearch. Вы можете добавить несколько подключений к серверу Elasticsearch или удалить подключение к серверу Elasticsearch. Для добавления подключения к серверу Elasticsearch нажмите на кнопку **+ Добавить подключение**. Для удаления подключения к серверу Elasticsearch нажмите рядом с ним на значок удаления ✕.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Коннектор, тип office365

Коннекторы с типом **office365** используются для получения данных Microsoft 365 (Office 365) по API.

Доступные параметры коннектора с типом **office365** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **office365**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Типы контента Office365	Типы контента, которые вы хотите получать в Kaspersky SIEM Cloud. Доступны следующие типы контента с информацией о действиях и событиях в Microsoft 365, сгруппированные в зависимости от источника информации: • **Audit.General**. • **Audit.AzureActiveDirectory**. • **Audit.Exchange**. • **Audit.Sharepoint**. • **DLP.All**. С подробной информацией о свойствах доступных типов контента и связанных с ними событиях можно ознакомиться на схеме на сайте Microsoft. Обязательный параметр. Можно выбрать один или несколько типов контента.
Идентификатор тенанта Office365	Уникальный идентификатор, получаемый после регистрации учетной записи в Microsoft 365. Если у вас его нет, обратитесь к вашему администратору или в Microsoft. Обязательный параметр.
ID клиента Office365	Уникальный идентификатор, получаемый после регистрации учетной записи в Microsoft 365. Если у вас его нет, обратитесь к вашему администратору или в Microsoft. Обязательный параметр.
Авторизация	Способ авторизации для подключения к Microsoft 365. Доступны следующие способы авторизации: • **PFX**. Использование секрета PFX. • **Токен**. Использование секрета token. Подробную информацию можно найти в разделе о секретах.
Учетные данные Office365	Поле становится доступно после выбора способа авторизации. Можно выбрать один из доступных секретов для авторизации или создать новый секрет выбранного типа. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
Хост для аутентификации	URL, по которому будет выполняться подключение и авторизация. По умолчанию выполняется подключение по адресу https://login.microsoftonline.com.
Хост ресурса	URL, откуда будут получены события. По умолчанию применяется адрес https://manage.office.com.
Интервал ретроспективного анализа, часы	Период, за который запрашиваются все новые события, в часах. Для избежания потери некоторых событий важно задавать перекрывающиеся интервалы получения событий, так как некоторые типы контента Microsoft 365 могут передаваться с задержкой. При этом ранее полученные события не дублируются. По умолчанию запрашиваются все новые события за последние 12 часов.
Время ожидания ответа, сек	Период ожидания ответа на запрос на получение новых событий в секундах. По умолчанию время ожидания ответа составляет 30 секунд.

Параметр	Описание
Интервал повтора, сек	Время, через которое необходимо повторить запрос на получение новых событий в случае ошибки, в секундах. По умолчанию запрос на получение новых событий повторяется через 10 секунд после получения ошибки или при отсутствии ответа в течение заданного времени ожидания.
Интервал очищения, сек	Периодичность удаления устаревших данных в секундах. Минимальное значение – 300 секунд. По умолчанию устаревшие данные удаляются каждые 1800 секунд.
Интервал запросов, мин	Периодичность отправки запросов на получение новых событий в минутах. По умолчанию запросы отправляются каждые 10 минут.
Прокси-сервер	Параметры прокси-сервера, если он требуется для подключения к Microsoft 365. Можно выбрать один из доступных или создать новый прокси-сервер.

Коннектор, тип dfi

Коннекторы с типом **dfi** используются для получения данных Kaspersky Digital Footprint Intelligence по API. Доступные параметры коннектора с типом **dfi** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **dfi**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.

URL	URL-адрес API сервиса Kaspersky Threat Intelligence Portal. В URL-адресе вам нужно указать имя хоста и номер порта или только имя хоста. Вы можете указать только один URL-адрес. Адрес Kaspersky TIP: https://tip.kaspersky.com/api.
	Поддерживаются следующие форматы URL-адресов:
	• `host name:port number` или `host name`;
	Примеры:
	`http://tip_hostname:2134/api`
	`http://tip_hostname/api`
	• `IPv4 address:port number` или `IPv4 address`;
	Примеры:
	`http://127.0.0.1:2134/api`
	`http://127.0.0.1/api`
	• `[IPv6 address]:port number` или `[IPv6 address]`.
	IPv6-адрес должен быть указан в квадратных скобках. Примеры:
	`http://[1050:0:0:0:5:600:300c:326b]:2134/api`
	`http://[1050:0:0:0:5:600:300c:326b]/api`.
	Kaspersky SIEM Cloud не позволяет сохранить ресурс или сервис, если в поле URL есть знак табуляции или пробел.
	Обязательный параметр.

Параметр	Описание
Секрет	Секрет, в котором хранятся учетные данные для подключения к серверу Kaspersky Threat Intelligence Portal. Вы можете выбрать существующий секрет или создать новый секрет. Для создания секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать секрет?** *Чтобы создать секрет:* 1. В поле **Название** введите название секрета. 2. В поле **Токен** укажите API-токен для аутентификации на портале Kaspersky Threat Intelligence Portal. Подробную информацию о получении API-токена вы найдете в справке Kaspersky Threat Intelligence Portal. 3. При необходимости с поле **Теги** добавьте теги для маркировки секрета. 4. При необходимости в поле **Описание** введите описание секрета. 5. Нажмите на кнопку **Создать**. Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**. Обязательный параметр.
Интервал запросов	Интервал запросов к сервису Kaspersky Digital Footprint Intelligence, в секундах. Укажите число от 60 до 3600 (то есть от 1 минуты до 60 минут). Значение по умолчанию: `120`. Обязательный параметр.
Начальная временная метка	Дата и время, начиная с которого сервис Kaspersky Digital Footprint Intelligence сформирует данные по запросу. По умолчанию запрос в Kaspersky Digital Footprint Intelligence формируется с данными за последние 30 дней до момента запуска коллектора. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Прокси-сервер	Параметры прокси-сервера, если он требуется для подключения к серверу Kaspersky Threat Intelligence Portal. Можно выбрать один из доступных или создать новый прокси-сервер. По умолчанию прокси-сервер не используется.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.

Коннектор, тип universalAPI

Коннекторы с типом **universalAPI** используются для получения данных из любых REST API, поддерживающих ответы в формате JSON.

Коннектор этого типа предназначен для работы только с теми REST API, которые могут быть сконфигурированы средствами пользовательского интерфейса. В рамках одного коннектора можно создать только одно соединение. В рамках одного соединения можно настроить только один URL-адрес.

Для коннекторов типа **universalAPI** обычно используется нормализатор **json**. Однако такие коннекторы могут принимать ответы API не только в виде структуры JSON, но и в виде обычной строки или числа. Для обработки таких ответов вы можете использовать другие нормализаторы, например **regexp** или **kv**.

Коннектор **universalAPI** поддерживает сбор событий из структур JSON только с одним уровнем вложенности. Если структура ответа содержит вложенные списки (например, список объектов, внутри которых находится другой список объектов), сбор событий из таких списков средствами коннектора не поддерживается. В этом случае рекомендуется собирать данные верхнего уровня, а обработку вложенных структур выполнять на уровне нормализатора.

Коннектор **universalAPI** не передает в нормализатор пустые события, содержащие объект `{}` или `[]`.

Проверку соединения с источником можно выполнить после запуска коллектора, проанализировав его журналы. В случае возникновения проблем с соединением или авторизацией коллектор будет отображаться в разделе **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы** в желтом статусе.

Коннектор с типом **universalAPI** не заменяет собой другие существующие API-коннекторы, например **office365**.

Доступные параметры коннектора с типом **universalAPI** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **universalAPI**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.
URL	URL-адрес REST API сервера. Указывать протокол подключения (http или https) не нужно. Он определяется автоматически в зависимости от значения параметра `tlsMode`. Вы можете указать только один URL-адрес. Обязательный параметр.
Интервал запросов (сек.)	Интервал опросов заданного URL, в секундах. Укажите число от `60` до `86 400` (то есть от 1 минуты до 24 часов). Значение по умолчанию: `3600`.
HTTP метод	HTTP-метод запроса к API. Доступные значения: • **GET**. • **POST**. • **PUT**. • **DELETE**. Обязательный параметр.
Авторизация	Способ авторизации для подключения к API. Доступны следующие способы авторизации: • **Выключена**. Авторизация не используется. • **Обычная**. Авторизация по логину и паролю. Нужно использовать секрет типа **credentials**. • **Токен**. Авторизация по токену. Нужно использовать секрет типа **token**. Подробную информацию можно найти в разделе о секретах. Значение по умолчанию: **Выключена**. Если на вкладке **Дополнительные параметры** в поле **Режим TLS** выбрано значение **Нестандартный PFX**, поле **Авторизация** будет недоступно.
Идентификатор секрета	Поле доступно, если в поле **Авторизация** выбрано значение **Обычная**. Нужно выбрать секрет типа **credentials**. Обязательный параметр.
Токен	Поле доступно, если в поле **Авторизация** выбрано значение **Token**. Нужно выбрать секрет типа **token**. Обязательный параметр.
Название токена	Поле доступно, если в поле **Авторизация** выбрано значение **Token**. Доступные значения: • **Bearer**. • **OAuth**. Вы также можете указать название вручную. Обязательный параметр.

Параметр	Описание
Тело запроса	Тело HTTP-запроса. Вы можете также использовать переменные: `$token`, `$username`, `$password`, `$identityValue`.
Путь к данным в формате JSONPath	Путь к данным в структуре ответа API, указывающий на объект или список объектов. Путь задается в формате JSONPath (например, `$.data`, `$.data.edges[0].node.event`, `$.data.edges[*].node.event`). Если в ответе API ожидается обычная строка или число, укажите в качестве пути символ `$`. Если при этом будет выключен параметр **Поле Identity** и не будут настроены параметры итераций, то данные будут переданы в нормализатор без изменения. Обязательный параметр.
Поле Identity	Переключатель для включения уникального идентификатора, по которому будут отбираться события. По умолчанию переключатель выключен.
Путь к полю в формате JSONPath	Поле доступно, если переключатель **Поле Identity** включен. Путь к полю идентификатора в структуре элемента данных ответа API задается в формате JSONPath (например, `$.id`). Обязательный параметр.
Тип	Поле доступно, если переключатель **Поле Identity** включен. Тип поля идентификатора, по которому будут отбираться события. Доступные значения: • **int**. • **float**. • **string**. • **date**. Внутри системы значение хранится в виде метки времени в миллисекундах. Обязательный параметр.
Формат даты	Поле доступно, если в поле **Тип** выбрано значение **date**. Формат даты может содержать дату, время, доли секунды и временную зону, например `YYYY-MM-DDTHH:mm:ssX`. Заданный формат применяется: • Для парсинга начального значения идентификатора. • Для парсинга значений идентификатора из ответов REST API. Если формат даты содержит временную зону, значение обрабатывается в указанной временной зоне. Если формат даты не содержит временную зону, значение обрабатывается в UTC. • Для формирования строки даты для параметров запроса (например, `$identityValue` в `queryParams`, `headers`, `body`). Если формат даты содержит временную зону, строка формируется во временной зоне сервера. Если формат даты не содержит временную зону, строка формируется в UTC.
Начальное значение	Поле доступно, если переключатель **Поле Identity** включен. Начальное значение поля идентификатора задается в виде строки в формате, соответствующем выбранному типу в поле **Тип**. Для типа **date** нужно указать значение в формате, указанном в поле **Формат даты**. Значение может содержать символы Unicode. Минимальная длина – 1 символ.
Параметры итераций	Переключатель для включения режима итераций, используемого для API с поэтапной выдачей данных. По умолчанию переключатель выключен.
Путь к полю с ключом итерации в формате JSONPath	Путь к полю ключа итерации в структуре элемента ответа API в формате JSONPath. Обязательный параметр.
Интервал запросов в режиме итераций (сек.)	Интервал опроса URL в режиме итерации, в секундах. Максимальное значение: `86 400` (24 часа). Значение по умолчанию: `60`.
Параметр URL для ключа итерации	Имя параметра URL, в котором передается ключ итерации при запросе к API.
Необязательные параметры запроса	Дополнительные параметры запроса в формате `map[string][]string`. Вы можете также использовать переменные: `$token`, `$username`, `$password`, `$identityValue`. Для добавления параметра нажмите на кнопку **+ Добавить** и заполните поля **Ключ** и **Значение**. Для удаления параметра установите рядом с ним флажок и нажмите на кнопку **Удалить**. Если включена итерация и в состоянии есть ключ итерации, он автоматически подставляется в параметры запроса.

Параметр	Описание
Заголовки запроса	Опциональные заголовки HTTP-запроса в формате `map[string][]string`. Вы можете также использовать переменные: `$token`, `$username`, `$password`, `$identityValue`. Для добавления параметра нажмите на кнопку **+ Добавить** и заполните поля **Ключ** и **Значение**. Для удаления параметра установите рядом с ним флажок и нажмите на кнопку **Удалить**.
Дополнительные поля	Дополнительные поля, которые добавляются в каждый элемент данных, в формате `map[string][]string`. Для добавления полей нажмите на кнопку **+ Добавить** и заполните поля **Название поля** и **JSONPath**. Для удаления поля установите рядом с ним флажок и нажмите на кнопку **Удалить**.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий режим отладки для коннектора. По умолчанию выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение **UTF-8**.
Прокси-сервер	Параметры прокси-сервера, если он требуется для подключения к API. Можно выбрать один из доступных прокси или создать новый.

Параметр	Описание

Режим TLS	Режим шифрования TLS. При использовании шифрования TLS вы не можете указать IP-адрес в поле **URL** на вкладке **Основные параметры**. Доступные значения:
	• **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию.
	• **Включено** – использовать шифрование TLS, но без верификации сертификатов.
	• **Нестандартный CA** – использовать шифрование TLS с верификацией сертификата, подписанного центром сертификации. При выборе этого значения в раскрывающемся списке **Нестандартный CA** укажите секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать сертификат, подписанный центром сертификации?
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра Kaspersky SIEM Cloud (в примерах команд ниже используется OpenSSL).
	Чтобы создать сертификат, подписанный центром сертификации:
	1. Создайте ключ, который будет использоваться центром сертификации, например:
	`openssl genrsa -out ca.key 2048`
	2. Создайте сертификат для созданного ключа, например:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<common name of the certification authority host>" -out ca.crt`
	3. Создайте приватный ключ и запрос на его подписание в центре сертификации, например:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<common host name of the Kaspersky SIEM Cloud server>" -out server.csr`
	4. Создайте сертификат, подписанный центром сертификации. Вам нужно включить в переменную `subjectAltName` доменные имена или IP-адреса сервера, для которого вы создаете сертификат, например:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Загрузите созданный сертификат `server.crt` в веб-интерфейсе Kaspersky SIEM Cloud в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	• **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс Kaspersky SIEM Cloud в виде PFX-секрета. При выборе этого значения в раскрывающемся списке **Нестандартный PFX** укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать PFX-секрет
	Чтобы создать PFX-секрет:
	1. В поле **Название** введите название PFX-секрета.
	2. Нажмите на кнопку **Загрузить PFX** и выберите файл в формате PKCS#12-контейнера, в который вы экспортировали файл PFX с закрытым ключом.
	3. В поле **Пароль** введите пароль для защиты файла PFX, указанный в мастере экспорта PFX.
	4. Нажмите на кнопку **Создать**.
	PFX-секрет будет создан и отобразится в раскрывающемся списке **PFX секрет**.

Время ожидания запроса (сек.)	Период ожидания ответа на запрос к API, в секундах. По умолчанию время ожидания ответа составляет 30 секунд.
Количество повторных запросов	Количество повторных попыток выполнить запрос при появлении ошибки. Значение по умолчанию: `1`.
Интервал повторных запросов (сек.)	Интервал между повторными попытками запроса, в секундах. Значение по умолчанию: `0`.

Коннектор, тип smb

Коннекторы с типом **smb** используются для получения данных по протоколу SMB (Server Message Block) при работе с агентами Linux. Доступные параметры коннектора с типом **smb** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип коннектора – **smb**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
URL	Путь до удаленной директории в одном из форматов: • `smb://<IP address or host_name>:<port>/<share_name>` • `smb://<IP address or host_name>:<port>/<share_name>/<path_to_directory>` Kaspersky SIEM Cloud получает информацию только из файлов, хранящихся в последней директории, указанной в пути. Например, вы указываете следующий путь: `smb://<IP address or host_name>:<port>/<share_name>/<directory_name1>/<directory_name2>` В таком случае Kaspersky SIEM Cloud получит информацию только из файлов из директории 2. Если в директории 2 хранятся вложенные директории, файлы из них прочитаны не будут. Если порт не указан, Kaspersky SIEM Cloud автоматически подставит порт 445. Обязательный параметр.
Маска имени файла	Маска, по которой фильтруются файлы с событиями. Допустимо использование масок "`*`", "`?`", "`[...]`". Пример: *.json Обязательный параметр.
Секрет	Секрет, в котором хранятся учетные данные для подключения к серверу SMB. Поддерживаются секреты с типом **credetials**. Аутентификация происходит по протоколу NTLMv2. Вы можете выбрать существующий секрет или создать новый секрет. Для создания секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша ✎. **Как создать секрет?** *Чтобы создать секрет:* 1. В поле **Название** введите название секрета. 2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору. 3. При необходимости в поле **Описание** введите описание секрета. 4. Нажмите на кнопку **Создать**. Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**. Обязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Минимальное значение: 16. Максимальное значение: 67 108 864 (64 МБ). Размер буфера по умолчанию: 1 048 576 (1 МБ), в интерфейсе отображается как **Авто**.
Количество обработчиков	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Интервал запросов, мс	Интервал (в миллисекундах), определяющий, как часто коннектор перечитывает файлы в директории. Значение по умолчанию: `0`. При этом значении коннектор перечитывает файлы в директории каждые 700 миллисекунд.
Кодировка символов	Кодировка файлов, полученных с SMB-сервера. По умолчанию используется кодировка UTF-8. Обязательный параметр.

Коннектор, тип http-streaming

Коннекторы с типом **http-streaming** используются для получения событий по протоколу HTTP при работе с агентами Windows и Linux.

Коннектор принимает HTTP-запросы и обрабатывает их тела следующим образом: читает и при необходимости декомпрессирует тело запроса, разделяет его на события и передает события на обработку по одному. Такой способ обработки позволяет снизить потребление памяти, однако может снижать производительность коннектора при высокой скорости поступления событий от небольшого количества источников.

Доступные параметры коннектора с типом **http-streaming** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя коннектора. Максимальная длина названия составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит коннектор. Обязательный параметр.
Тип	Тип коннектора – **http-streaming**. Обязательный параметр.
Теги	Теги для поиска коннектора. Необязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Вы можете ввести URL-адрес в одном из следующих форматов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address>:<port number>`; Для того чтобы данные из источника событий отправлялись в коннектор, указанный вами URL-адрес должен оканчиваться на `/input`. Обязательный параметр.
Разделитель	Символ, определяющий границу между событиями: • **\n**; • **\t**; • **\0**. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений.

Параметр	Описание
Размер буфера	Определяет максимальный размер одного события в байтах. Максимальный размер события составляет1 байт. Если в теле HTTP-запроса отсутствуют разделители, все тело запроса считается одним событием. В этом случае размер буфера должен быть больше размера тела запроса. Рекомендуется устанавливать размер буфера исходя из размера самого объемного события, а не размера пачки событий, с запасом не менее 2 байт. Значение по умолчанию: 4096 байт (4 КБ). Максимальное значение: 67108864 байт (64 МБ). Если указано значение 0, используется значение по умолчанию.
Описание	Описание коннектора. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Отладка	Переключатель, включающий запись работы ресурса в журнал. По умолчанию переключатель выключен.
Кодировка символов	Кодировка символов. По умолчанию выбрано значение UTF-8.
Режим TLS	Режим шифрования TLS. При использовании шифрования TLS вы не можете указать IP-адрес в поле URL на вкладке **Основные параметры**. Доступные значения: • **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию. • **Включено** – использовать шифрование TLS, но без верификации сертификатов. • **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс Kaspersky SIEM Cloud в виде PFX-секрета. При выборе этого значения в раскрывающемся списке **Нестандартный PFX с аутентификацией клиента** укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать PFX-секрет?** *Чтобы создать PFX-секрет:* 1. В поле **Название** введите название PFX-секрета. 2. Нажмите на кнопку **Загрузить PFX** и выберите файл в формате PKCS#12-контейнера, в который вы экспортировали файл PFX с закрытым ключом. 3. В поле **Пароль** введите пароль для защиты файла PFX, указанный в мастере экспорта PFX. 4. Нажмите на кнопку **Создать**. PFX-секрет будет создан и отобразится в раскрывающемся списке **PFX секрет**. • **Нестандартный PFX с аутентификацией клиента** – использовать шифрование TLS с PFX-секретом. В этом режиме выполняется аутентификация клиента по сертификату. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс Kaspersky SIEM Cloud в виде PFX-секрета. При выборе этого значения в раскрывающемся списке **Нестандартный PFX с аутентификацией клиента** укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать PFX-секрет?** *Чтобы создать PFX-секрет:* 1. В поле **Название** введите название PFX-секрета. 2. Нажмите на кнопку **Загрузить PFX** и выберите файл в формате PKCS#12-контейнера, в который вы экспортировали файл PFX с закрытым ключом. 3. В поле **Пароль** введите пароль для защиты файла PFX, указанный в мастере экспорта PFX. 4. Нажмите на кнопку **Создать**. PFX-секрет будет создан и отобразится в раскрывающемся списке **PFX секрет**.

Параметр	Описание
Число входящих запросов в очереди	Максимальное количество HTTP-запросов, которые коннектор обрабатывает одновременно. При достижении установленного ограничения новые HTTP-запросы отклоняются с кодом `429 Too Many Requests`. Тело отклоненного запроса не обрабатывается. Фактическое количество одновременно обрабатываемых запросов зависит от значения этого параметра и количества обработчиков сервиса, заданного в коллекторе параметром **Обработчики**. Значение по умолчанию: 32768. Максимальное значение: 65535. Если указано значение 0, используется значение по умолчанию. Увеличение значения позволяет обрабатывать больше запросов одновременно, но может привести к увеличению потребления памяти.

Предустановленные коннекторы

В поставку Kaspersky SIEM Cloud включены перечисленные в таблице предустановленные коннекторы.

Предустановленные коннекторы

Название коннектора	Комментарий
[OOTB] Continent SQL	Собирает события из СУБД АПКШ Континент. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] InfoWatch Person Monitor SQL	Собирает системные события аудита из СУБД MS SQL системы InfoWatch Person Monitor версии 10.2.
[OOTB] InfoWatch Traffic Monitor SQL	Собирает события из СУБД системы InfoWatch Traffic Monitor. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] Kaspersky Security for MS Exchange Server SQL	Собирает события из СУБД MS SQL системы Kaspersky Security для Microsoft Exchange Servers версии 9.0. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] KSC MSSQL	Собирает события из СУБД MS SQL системы Open Single Management Platform. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] KSC MySQL	Собирает события из СУБД MySQL системы Open Single Management Platform. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] KSC PostgreSQL	Собирает события из СУБД PostgreSQL системы Open Single Management Platform версии 15.0. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] Oracle Audit Trail SQL	Собирает события аудита из СУБД Oracle. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] Parsec ParsecNet MSSQL	Собирает события из СУБД MS SQL системы ParsecNET 3. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] SecretNet SQL	Собирает события из СУБД системы SecretNet SQL. Для использования необходимо настроить параметры соответствующего типа секрета.
[OOTB] TeamPass MySQL	Собирает события из СУБД MySQL системы TeamPass версии 3.1.
[OOTB] Zabbix MySQL	Собирает события из СУБД MySQL системы Zabbix версии 6.4.

Использование точки назначения

Точки назначения задают сетевые параметры для передачи нормализованных событий. В коллекторах и коррелляторах точки назначения используются для описания того, куда передавать обработанные события. Как правило, в роли точек назначения выступают коррелятор и хранилище.

В поставку Kaspersky SIEM Cloud включены следующие предустановленные точки назначения, которые вы можете использовать при создании коллектора и коррелятора:

- [OOTB] Correlator – отправляет события в коррелятор.
- [OOTB] Storage – отправляет события в хранилище.

Чтобы создать точку назначения:

1. В веб-интерфейсе перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Точки назначения** и нажмите кнопку **Создать**.
2. На вкладке **Основные параметры** в поле **Название** введите уникальное имя точки назначения. Название должно содержать от 1 до 128 символов в кодировке Unicode.
3. С помощью переключателя **Состояние** вы можете включить или выключить сервис
4. В раскрывающемся списке **Тип** выберите тип точки назначения и настройте необходимые параметры на вкладках **Основные параметры** и **Дополнительные параметры** в зависимости от выбранного типа:
   - internal
   - nats-jetstream
   - tcp
   - udp
   - http
   - diode
   - kafka
   - file
   - storage
   - correlator
   - eventRouter
5. Нажмите кнопку **Создать**.

Точка назначения, тип internal

Точки назначения с типом **internal** используются для приема данных от сервисов Kaspersky SIEM Cloud по протоколу internal. Вы можете передавать следующие данные по протоколу internal:

- Внутренние данные, такие как маршруты событий.
- Файловые атрибуты. Если при создании коллектора на шаге Транспорт мастера установки вы указали коннектор с типом file, на шаге **Парсинг событий** в таблице **Сопоставление** вы можете передать в поле события Kaspersky SIEM Cloud название обрабатываемого коллектором файла или путь к файлу. Для этого в столбце **Исходные данные** укажите одно из следующих значений:
  - `$kuma_fileSourceName` – передать в поле события Kaspersky SIEM Cloud название обрабатываемого коллектором файла.
  - `$kuma_fileSourcePath` – передать в поле события Kaspersky SIEM Cloud путь к обрабатываемому коллектором файлу.

  Когда вы используете коннектор с типом **file**, новые переменные в нормализаторе будут работать только с точками назначения с типом **internal**.
- События в маршрутизатор событий. Для отправки событий в маршрутизатор событий используются точки назначения с типом **internal**. Маршрутизатор событий также имеет собственный тип **eventRouter**, который используется для соответствующей настройки маршрутизатора.

Доступные параметры точки назначения с типом **internal** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Состояние	Переключатель, включающий отправку событий в точку назначения. По умолчанию этот переключатель включен.
Тип	Тип точки назначения – **internal**. Обязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Поддерживаются следующие форматы URL-адресов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address><port number>`. IPv6-адреса можно указать в формате `[<IPv6 address>%<interface>:<port number>`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Вы можете добавить несколько URL-адресов и удалить URL-адрес. Kaspersky SIEM Cloud не позволяет сохранить ресурс или сервис если в поле URL есть знак табуляции или пробел. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 16777216 (16 МБ), в интерфейсе отображается как 0.
Интервал очистки буфера	Интервал в секундах для отправки событий в точку назначения. Значение по умолчанию: 1 секунда.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию: 10 ГБ, в интерфейсе отображается как 0.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Прокси-сервер	Прокси-сервер для точки назначения. Вы можете выбрать существующий прокси-сервер или создать новый прокси-сервер. Для создания нового прокси-сервера выберите **Создать**. Если вы хотите изменить параметры существующего прокси-сервера, нажмите рядом с ним на значок карандаша.
Сжатие	Определяет, будет ли поток событий, отправляемый агентом Kaspersky SIEM Cloud в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
Политика выбора URL	Способ определения URL-адресов, на которые события отправляются в первую очередь, если вы добавили несколько URL-адресов в поле **URL** на вкладке **Основные параметры**: • **Любой** – события отправляются на случайно выбранный доступный URL-адрес до тех пор, пока URL-адрес принимает события. Если URL-адрес станет недоступным, события будут отправляться на другой случайно выбранный доступный URL-адрес. Это значение выбрано по умолчанию. • **Сначала первый** – события отправляются на первый добавленный URL-адрес. Если URL-адрес станет недоступным, события будут отправляться на следующий добавленный доступный URL-адрес. Если первый добавленный URL-адрес снова станет доступным, события будут отправляться на него. • **Сбалансированный** – события равномерно распределяются между доступными URL-адресами. Этот способ определения URL-адресов не гарантирует равномерного распределения событий по URL-адресам, так как буфер может быть переполнен или события могут быть отправлены в точку назначения. Вы можете указать размер буфера в байтах в поле **Размер буфера**, а также указать интервал в секундах для отправки событий в точку назначения в поле **Интервал очистки буфера**.
Ожидание проверки работоспособности	Интервал в секундах для проверки работоспособности точки назначения.
Дисковый буфер	Переключатель, включающий использование дискового буфера. По умолчанию этот переключатель включен. Дисковый буфер используется, если коллектор не может отправить в точку назначения нормализованные события. Вы можете указать размер дискового буфера в поле **Размер дискового буфера**. Если в дисковом буфере не останется свободного пространства, новые нормализованные события будут перезаписывать старые нормализованные события, начиная с самого старого.
Время ожидания	Время в секундах, в течение которого точка назначения ожидает ответа другого сервиса или компонента.
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.

Параметр	Описание
Фильтр	Фильтр для определения событий, которые будут обрабатываться ресурсом. Вы можете выбрать существующий фильтр или создать новый фильтр. Для создания нового фильтра выберите значение **Создать**. Если вы хотите изменить параметры существующего фильтра, нажмите рядом с ним на значок карандаша. **Как создать фильтр?** Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. Выберите режим создания фильтра: **Конструктор** или **Код**. При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра. 5. Если вы выбрали вариант **Конструктор**, выполните следующие действия: a. В раскрывающемся списке выберите логический оператор: • **И** – отбирает события, которые соответствуют всем указанным условиям. • **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий. • **НЕ** – отбирает события, которые не соответствуют всем указанным условиям. b. Нажмите на кнопку **Добавить условие**. c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра. **Операнды фильтров** • **Поля событий** – поле события, которое требуется использовать как операнд фильтра. • **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**. Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра. • **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – словарь, который требуется использовать. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря. • **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события. • **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать. • **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы. • **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда. • **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда. • **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.

Параметр	Описание

	• **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
	  • **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
	  • **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
	  • **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
	• **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константа, которую требуется присвоить операнду.
	• **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
	Операторы фильтров
	• **=** – левый операнд равен правому операнду.
	• **<** – левый операнд меньше правого операнда.
	• **<=** – левый операнд меньше или равен правому операнду.
	• **>** – левый операнд больше правого операнда.
	• **>=** – левый операнд больше или равен правому операнду.
	• **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
	• **contains** – левый операнд содержит значения правого операнда.
	• **startsWith** – левый операнд начинается с одного из значений правого операнда.
	• **endsWith** – левый операнд заканчивается одним из значений правого операнда.
	• **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
	• **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).
	Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.
	Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
	• **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
	Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
	• **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
	• **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
	• **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
	• **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
	• **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись.
	• **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.
	Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.
	Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.
	e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.
	Вы можете добавить несколько групп условий.
	6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.
	В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

Параметр	Описание
	7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕. 8. Нажмите **Сохранить**.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису → Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип nats-jetstream

Точки назначения с типом **nats-jetstream** используются для коммуникации через NATS. Доступные параметры точки назначения с типом **nats-jetstream** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Состояние	Переключатель, включающий отправку событий в точку назначения. По умолчанию этот переключатель включен.
Тип	Тип точки назначения – **nats-jetstream**. Обязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Поддерживаются следующие форматы URL-адресов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address><port number>`. IPv6-адреса можно указать в формате `[<IPv6 address>%<interface>:<port number>`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Вы можете добавить несколько URL-адресов и удалить URL-адрес. Kaspersky SIEM Cloud не позволяет сохранить ресурс или сервис если в поле URL есть знак табуляции или пробел. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр.
Тема	Тема сообщений NATS. Символы вводятся в кодировке Unicode. Обязательный параметр.

Параметр	Описание
Авторизация	Тип авторизации при подключении к URL-адресу, указанному в поле **URL**. • **Выключена**. Это значение выбрано по умолчанию. • **Обычная**. Этот тип авторизации осуществляется с помощью механизма SASL/PLAIN, который передает имя пользователя и пароль в открытом виде. Как правило, для обеспечения безопасности передачи данных (шифрования) в SASL/PLAIN используется TLS. При выборе этого значения в раскрывающемся списке **Секрет** укажите секрет, содержащий учетные данные пользователя для авторизации при подключении к точке назначения. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать секрет?** *Чтобы создать секрет:* 1. В поле **Название** введите название секрета. 2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору. 3. При необходимости в поле **Описание** введите описание секрета. 4. Нажмите на кнопку **Создать**. Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Интервал очистки буфера	Интервал в секундах для отправки событий в точку назначения. Значение по умолчанию: 1 секунда.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию: 10 ГБ, в интерфейсе отображается как 0.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Выходной формат	Формат, в котором события отправляются во внешний источник: • **JSON**. • **CEF**. При выборе этого значения в отправляемых событиях содержится заголовок CEF и только поля с непустыми значениями. • **Syslog-CEF**.

Параметр	Описание

Режим TLS	Режим шифрования TLS. При использовании шифрования TLS вы не можете указать IP-адрес в поле **URL** на вкладке **Основные параметры**. Доступные значения:
	• **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию.
	• **Включено** – использовать шифрование TLS, но без верификации сертификатов.
	• **Нестандартный CA** – использовать шифрование TLS с верификацией сертификата, подписанного центром сертификации. При выборе этого значения в раскрывающемся списке **Нестандартный CA** укажите секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать сертификат, подписанный центром сертификации?
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра Kaspersky SIEM Cloud (в примерах команд ниже используется OpenSSL).
	Чтобы создать сертификат, подписанный центром сертификации:
	1. Создайте ключ, который будет использоваться центром сертификации, например:
	`openssl genrsa -out ca.key 2048`
	2. Создайте сертификат для созданного ключа, например:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<common name of the certification authority host>" -out ca.crt`
	3. Создайте приватный ключ и запрос на его подписание в центре сертификации, например:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<common host name of the Kaspersky SIEM Cloud server>" -out server.csr`
	4. Создайте сертификат, подписанный центром сертификации. Вам нужно включить в переменную `subjectAltName` доменные имена или IP-адреса сервера, для которого вы создаете сертификат, например:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Загрузите созданный сертификат `server.crt` в веб-интерфейсе Kaspersky SIEM Cloud в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	Для использования сертификатов Kaspersky SIEM Cloud на сторонних устройствах вам нужно изменить расширение файла сертификата с CERT на CRT. В противном случае вы можете получить ошибку `x509: certificate signed by unknown authority`.
	• **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс Kaspersky SIEM Cloud в виде PFX-секрета. При выборе этого значения в раскрывающемся списке **PFX секрет** укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать PFX-секрет?
	Чтобы создать PFX-секрет:
	1. В поле **Название** введите название PFX-секрета.
	2. Нажмите на кнопку **Загрузить PFX** и выберите файл в формате PKCS#12-контейнера, в который вы экспортировали файл PFX с закрытым ключом.
	3. В поле **Пароль** введите пароль для защиты файла PFX, указанный в мастере экспорта PFX.
	4. Нажмите на кнопку **Создать**.
	PFX-секрет будет создан и отобразится в раскрывающемся списке **PFX секрет**.
	Режим **Нестандартный PFX** не отображается, если для параметра **Авторизация** выбрано значение **Обычная**.

Сжатие	Определяет, будет ли поток событий, отправляемый агентом Kaspersky SIEM Cloud в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.

Параметр	Описание
Разделитель	Символ, определяющий границу между событиями: • **\n**; • **\t**; • **\0**. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений.
Дисковый буфер	Переключатель, включающий использование дискового буфера. По умолчанию этот переключатель включен. Дисковый буфер используется, если коллектор не может отправить в точку назначения нормализованные события. Вы можете указать размер дискового буфера в поле **Размер дискового буфера**. Если в дисковом буфере не останется свободного пространства, новые нормализованные события будут перезаписывать старые нормализованные события, начиная с самого старого.
Время ожидания	Время в секундах, в течение которого точка назначения ожидает ответа другого сервиса или компонента.
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.

Параметр	Описание
Фильтр	Фильтр для определения событий, которые будут обрабатываться ресурсом. Вы можете выбрать существующий фильтр или создать новый фильтр. Для создания нового фильтра выберите значение **Создать**. Если вы хотите изменить параметры существующего фильтра, нажмите рядом с ним на значок карандаша. **Как создать фильтр?** Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. Выберите режим создания фильтра: **Конструктор** или **Код**. При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра. 5. Если вы выбрали вариант **Конструктор**, выполните следующие действия: a. В раскрывающемся списке выберите логический оператор: • **И** – отбирает события, которые соответствуют всем указанным условиям. • **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий. • **НЕ** – отбирает события, которые не соответствуют всем указанным условиям. b. Нажмите на кнопку **Добавить условие**. c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра. **Операнды фильтров** • **Поля событий** – поле события, которое требуется использовать как операнд фильтра. • **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**. Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра. • **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – словарь, который требуется использовать. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря. • **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события. • **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать. • **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы. • **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда. • **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда. • **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.

Параметр	Описание

	• **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
	  • **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
	  • **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
	  • **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
	• **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константа, которую требуется присвоить операнду.
	• **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
	Операторы фильтров
	• **=** – левый операнд равен правому операнду.
	• **<** – левый операнд меньше правого операнда.
	• **<=** – левый операнд меньше или равен правому операнду.
	• **>** – левый операнд больше правого операнда.
	• **>=** – левый операнд больше или равен правому операнду.
	• **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
	• **contains** – левый операнд содержит значения правого операнда.
	• **startsWith** – левый операнд начинается с одного из значений правого операнда.
	• **endsWith** – левый операнд заканчивается одним из значений правого операнда.
	• **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
	• **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).
	Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.
	Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
	• **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
	Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
	• **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
	• **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
	• **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
	• **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
	• **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в коррелляторах.
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись.
	• **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.
	Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.
	Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.
	e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.
	Вы можете добавить несколько групп условий.
	6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.
	В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

Параметр	Описание
	7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕. 8. Нажмите **Сохранить**.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису → Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип tcp

Точки назначения с типом **tcp** используются для связи по протоколу TCP. Доступные параметры точки назначения с типом **tcp** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Состояние	Переключатель, включающий отправку событий в точку назначения. По умолчанию этот переключатель включен.
Тип	Тип точки назначения – **tcp**. Обязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Поддерживаются следующие форматы URL-адресов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address><port number>`. IPv6-адреса можно указать в формате `[<IPv6 address>%<interface>:<port number>`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Вы можете добавить несколько URL-адресов и удалить URL-адрес. Kaspersky SIEM Cloud не позволяет сохранить ресурс или сервис если в поле URL есть знак табуляции или пробел. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Интервал очистки буфера	Интервал в секундах для отправки событий в точку назначения. Значение по умолчанию: 1 секунда.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию: 10 ГБ, в интерфейсе отображается как 0.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Выходной формат	Формат, в котором события отправляются во внешний источник: • **JSON**. • **CEF**. При выборе этого значения в отправляемых событиях содержится заголовок CEF и только поля с непустыми значениями. • **Syslog-CEF**.
Режим TLS	Режим шифрования TLS. При использовании шифрования TLS вы не можете указать IP-адрес в поле **URL** на вкладке **Основные параметры**. Доступные значения: • **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию. • **Включено** – использовать шифрование TLS, но без верификации сертификатов.
Сжатие	Определяет, будет ли поток событий, отправляемый агентом Kaspersky SIEM Cloud в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
Политика выбора URL	Способ определения URL-адресов, на которые события отправляются в первую очередь, если вы добавили несколько URL-адресов в поле **URL** на вкладке **Основные параметры**: • **Любой** – события отправляются на случайно выбранный доступный URL-адрес до тех пор, пока URL-адрес принимает события. Если URL-адрес станет недоступным, события будут отправляться на другой случайно выбранный доступный URL-адрес. Это значение выбрано по умолчанию. • **Сначала первый** – события отправляются на первый добавленный URL-адрес. Если URL-адрес станет недоступным, события будут отправляться на следующий добавленный доступный URL-адрес. Если первый добавленный URL-адрес снова станет доступным, события будут отправляться на него. • **Сбалансированный** – события равномерно распределяются между доступными URL-адресами. Этот способ определения URL-адресов не гарантирует равномерного распределения событий по URL-адресам, так как буфер может быть переполнен или события могут быть отправлены в точку назначения. Вы можете указать размер буфера в байтах в поле **Размер буфера**, а также указать интервал в секундах для отправки событий в точку назначения в поле **Интервал очистки буфера**.
Разделитель	Символ, определяющий границу между событиями: • **\n**; • **\t**; • **\0**. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений.
Дисковый буфер	Переключатель, включающий использование дискового буфера. По умолчанию этот переключатель включен. Дисковый буфер используется, если коллектор не может отправить в точку назначения нормализованные события. Вы можете указать размер дискового буфера в поле **Размер дискового буфера**. Если в дисковом буфере не останется свободного пространства, новые нормализованные события будут перезаписывать старые нормализованные события, начиная с самого старого.
Время ожидания	Время в секундах, в течение которого точка назначения ожидает ответа другого сервиса или компонента.
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.

Параметр	Описание
Фильтр	Фильтр для определения событий, которые будут обрабатываться ресурсом. Вы можете выбрать существующий фильтр или создать новый фильтр. Для создания нового фильтра выберите значение **Создать**. Если вы хотите изменить параметры существующего фильтра, нажмите рядом с ним на значок карандаша. **Как создать фильтр?** Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. Выберите режим создания фильтра: **Конструктор** или **Код**. При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра. 5. Если вы выбрали вариант **Конструктор**, выполните следующие действия: a. В раскрывающемся списке выберите логический оператор: • **И** – отбирает события, которые соответствуют всем указанным условиям. • **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий. • **НЕ** – отбирает события, которые не соответствуют всем указанным условиям. b. Нажмите на кнопку **Добавить условие**. c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра. **Операнды фильтров** • **Поля событий** – поле события, которое требуется использовать как операнд фильтра. • **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**. Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра. • **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – словарь, который требуется использовать. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря. • **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события. • **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать. • **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы. • **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда. • **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда. • **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.

Параметр	Описание

	• **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
	  • **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
	  • **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
	  • **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
	• **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константа, которую требуется присвоить операнду.
	• **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
	Операторы фильтров
	• **=** – левый операнд равен правому операнду.
	• **<** – левый операнд меньше правого операнда.
	• **<=** – левый операнд меньше или равен правому операнду.
	• **>** – левый операнд больше правого операнда.
	• **>=** – левый операнд больше или равен правому операнду.
	• **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
	• **contains** – левый операнд содержит значения правого операнда.
	• **startsWith** – левый операнд начинается с одного из значений правого операнда.
	• **endsWith** – левый операнд заканчивается одним из значений правого операнда.
	• **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
	• **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).
	Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.
	Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
	• **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
	Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
	• **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
	• **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
	• **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
	• **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
	• **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись.
	• **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.
	Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.
	Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.
	e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.
	Вы можете добавить несколько групп условий.
	6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.
	В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

Параметр	Описание
	7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕. 8. Нажмите **Сохранить**.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису → Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип udp

Точки назначения с типом **udp** используются для связи по протоколу UDP. Доступные параметры точки назначения с типом **udp** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Состояние	Переключатель, включающий отправку событий в точку назначения. По умолчанию этот переключатель включен.
Тип	Тип точки назначения – **udp**. Обязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Поддерживаются следующие форматы URL-адресов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address><port number>`. IPv6-адреса можно указать в формате `[<IPv6 address>%<interface>:<port number>`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Вы можете добавить несколько URL-адресов и удалить URL-адрес. Kaspersky SIEM Cloud не позволяет сохранить ресурс или сервис если в поле URL есть знак табуляции или пробел. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Интервал очистки буфера	Интервал в секундах для отправки событий в точку назначения. Значение по умолчанию: 1 секунда.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию: 10 ГБ, в интерфейсе отображается как 0.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Выходной формат	Формат, в котором события отправляются во внешний источник: • **JSON**. • **CEF**. При выборе этого значения в отправляемых событиях содержится заголовок CEF и только поля с непустыми значениями. • **Syslog-CEF**.
Сжатие	Определяет, будет ли поток событий, отправляемый агентом Kaspersky SIEM Cloud в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
Политика выбора URL	Способ определения URL-адресов, на которые события отправляются в первую очередь, если вы добавили несколько URL-адресов в поле **URL** на вкладке **Основные параметры**: • **Любой** – события отправляются на случайно выбранный доступный URL-адрес до тех пор, пока URL-адрес принимает события. Если URL-адрес станет недоступным, события будут отправляться на другой случайно выбранный доступный URL-адрес. Это значение выбрано по умолчанию. • **Сначала первый** – события отправляются на первый добавленный URL-адрес. Если URL-адрес станет недоступным, события будут отправляться на следующий добавленный доступный URL-адрес. Если первый добавленный URL-адрес снова станет доступным, события будут отправляться на него. • **Сбалансированный** – события равномерно распределяются между доступными URL-адресами. Этот способ определения URL-адресов не гарантирует равномерного распределения событий по URL-адресам, так как буфер может быть переполнен или события могут быть отправлены в точку назначения. Вы можете указать размер буфера в байтах в поле **Размер буфера**, а также указать интервал в секундах для отправки событий в точку назначения в поле **Интервал очистки буфера**.
Разделитель	Символ, определяющий границу между событиями: • **\n**; • **\t**; • **\0**. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений.
Дисковый буфер	Переключатель, включающий использование дискового буфера. По умолчанию этот переключатель включен. Дисковый буфер используется, если коллектор не может отправить в точку назначения нормализованные события. Вы можете указать размер дискового буфера в поле **Размер дискового буфера**. Если в дисковом буфере не останется свободного пространства, новые нормализованные события будут перезаписывать старые нормализованные события, начиная с самого старого.
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.

Параметр	Описание
Фильтр	Фильтр для определения событий, которые будут обрабатываться ресурсом. Вы можете выбрать существующий фильтр или создать новый фильтр. Для создания нового фильтра выберите значение **Создать**. Если вы хотите изменить параметры существующего фильтра, нажмите рядом с ним на значок карандаша. **Как создать фильтр?** Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. Выберите режим создания фильтра: **Конструктор** или **Код**. При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра. 5. Если вы выбрали вариант **Конструктор**, выполните следующие действия: a. В раскрывающемся списке выберите логический оператор: • **И** – отбирает события, которые соответствуют всем указанным условиям. • **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий. • **НЕ** – отбирает события, которые не соответствуют всем указанным условиям. b. Нажмите на кнопку **Добавить условие**. c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра. **Операнды фильтров** • **Поля событий** – поле события, которое требуется использовать как операнд фильтра. • **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**. Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра. • **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – словарь, который требуется использовать. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря. • **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события. • **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать. • **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы. • **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда. • **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда. • **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.

Параметр	Описание

	• **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
	  • **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
	  • **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
	  • **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
	• **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константа, которую требуется присвоить операнду.
	• **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
	Операторы фильтров
	• **=** – левый операнд равен правому операнду.
	• **<** – левый операнд меньше правого операнда.
	• **<=** – левый операнд меньше или равен правому операнду.
	• **>** – левый операнд больше правого операнда.
	• **>=** – левый операнд больше или равен правому операнду.
	• **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
	• **contains** – левый операнд содержит значения правого операнда.
	• **startsWith** – левый операнд начинается с одного из значений правого операнда.
	• **endsWith** – левый операнд заканчивается одним из значений правого операнда.
	• **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
	• **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).
	Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.
	Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
	• **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
	Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
	• **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
	• **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
	• **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
	• **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
	• **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись.
	• **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.
	Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.
	Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.
	e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.
	Вы можете добавить несколько групп условий.
	6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.
	В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

Параметр	Описание
	7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕. 8. Нажмите **Сохранить**.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису → Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип http

Точки назначения с типом **http** используются для связи по протоколу HTTP. Доступные параметры точки назначения с типом **http** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Состояние	Переключатель, включающий отправку событий в точку назначения. По умолчанию этот переключатель включен.
Тип	Тип точки назначения – **http**. Обязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Поддерживаются следующие форматы URL-адресов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address><port number>`. IPv6-адреса можно указать в формате `[<IPv6 address>%<interface>:<port number>`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Вы можете добавить несколько URL-адресов и удалить URL-адрес. Kaspersky SIEM Cloud не позволяет сохранить ресурс или сервис если в поле URL есть знак табуляции или пробел. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр.

Параметр	Описание
Авторизация	Тип авторизации при подключении к URL-адресу, указанному в поле **URL**. • **Выключена**. Это значение выбрано по умолчанию. • **Обычная**. Этот тип авторизации осуществляется с помощью механизма SASL/PLAIN, который передает имя пользователя и пароль в открытом виде. Как правило, для обеспечения безопасности передачи данных (шифрования) в SASL/PLAIN используется TLS. При выборе этого значения в раскрывающемся списке **Секрет** укажите секрет, содержащий учетные данные пользователя для авторизации при подключении к точке назначения. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать секрет?** *Чтобы создать секрет:* 1. В поле **Название** введите название секрета. 2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору. 3. При необходимости в поле **Описание** введите описание секрета. 4. Нажмите на кнопку **Создать**. Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Интервал очистки буфера	Интервал в секундах для отправки событий в точку назначения. Значение по умолчанию: 1 секунда.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию: 10 ГБ, в интерфейсе отображается как 0.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Выходной формат	Формат, в котором события отправляются во внешний источник: • **JSON**. • **CEF**. При выборе этого значения в отправляемых событиях содержится заголовок CEF и только поля с непустыми значениями. • **Syslog-CEF**.

Параметр	Описание

Режим TLS	Режим шифрования TLS. При использовании шифрования TLS вы не можете указать IP-адрес в поле **URL** на вкладке **Основные параметры**. Доступные значения:
	• **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию.
	• **Включено** – использовать шифрование TLS, но без верификации сертификатов.
	• **Нестандартный CA** – использовать шифрование TLS с верификацией сертификата, подписанного центром сертификации. При выборе этого значения в раскрывающемся списке **Нестандартный CA** укажите секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать сертификат, подписанный центром сертификации?
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра Kaspersky SIEM Cloud (в примерах команд ниже используется OpenSSL).
	Чтобы создать сертификат, подписанный центром сертификации:
	1. Создайте ключ, который будет использоваться центром сертификации, например:
	`openssl genrsa -out ca.key 2048`
	2. Создайте сертификат для созданного ключа, например:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<common name of the certification authority host>" -out ca.crt`
	3. Создайте приватный ключ и запрос на его подписание в центре сертификации, например:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<common host name of the Kaspersky SIEM Cloud server>" -out server.csr`
	4. Создайте сертификат, подписанный центром сертификации. Вам нужно включить в переменную `subjectAltName` доменные имена или IP-адреса сервера, для которого вы создаете сертификат, например:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Загрузите созданный сертификат `server.crt` в веб-интерфейсе Kaspersky SIEM Cloud в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	Для использования сертификатов Kaspersky SIEM Cloud на сторонних устройствах вам нужно изменить расширение файла сертификата с CERT на CRT. В противном случае вы можете получить ошибку `x509: certificate signed by unknown authority`.
	• **Нестандартный PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера, после чего загрузить PFX-сертификат в веб-интерфейс Kaspersky SIEM Cloud в виде PFX-секрета. При выборе этого значения в раскрывающемся списке **PFX секрет** укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать PFX-секрет?
	Чтобы создать PFX-секрет:
	1. В поле **Название** введите название PFX-секрета.
	2. Нажмите на кнопку **Загрузить PFX** и выберите файл в формате PKCS#12-контейнера, в который вы экспортировали файл PFX с закрытым ключом.
	3. В поле **Пароль** введите пароль для защиты файла PFX, указанный в мастере экспорта PFX.
	4. Нажмите на кнопку **Создать**.
	PFX-секрет будет создан и отобразится в раскрывающемся списке **PFX секрет**.
	Режим **Нестандартный PFX** не отображается, если для параметра **Авторизация** выбрано значение **Обычная**.

Прокси-сервер	Прокси-сервер для точки назначения. Вы можете выбрать существующий прокси-сервер или создать новый прокси-сервер. Для создания нового прокси-сервера выберите **Создать**. Если вы хотите изменить параметры существующего прокси-сервера, нажмите рядом с ним на значок карандаша.

Параметр	Описание
Сжатие	Определяет, будет ли поток событий, отправляемый агентом Kaspersky SIEM Cloud в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
Политика выбора URL	Способ определения URL-адресов, на которые события отправляются в первую очередь, если вы добавили несколько URL-адресов в поле **URL** на вкладке **Основные параметры**: • **Любой** – события отправляются на случайно выбранный доступный URL-адрес до тех пор, пока URL-адрес принимает события. Если URL-адрес станет недоступным, события будут отправляться на другой случайно выбранный доступный URL-адрес. Это значение выбрано по умолчанию. • **Сначала первый** – события отправляются на первый добавленный URL-адрес. Если URL-адрес станет недоступным, события будут отправляться на следующий добавленный доступный URL-адрес. Если первый добавленный URL-адрес снова станет доступным, события будут отправляться на него. • **Сбалансированный** – события равномерно распределяются между доступными URL-адресами. Этот способ определения URL-адресов не гарантирует равномерного распределения событий по URL-адресам, так как буфер может быть переполнен или события могут быть отправлены в точку назначения. Вы можете указать размер буфера в байтах в поле **Размер буфера**, а также указать интервал в секундах для отправки событий в точку назначения в поле **Интервал очистки буфера**.
Разделитель	Символ, определяющий границу между событиями: • **\n**; • **\t**; • **\0**. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений.
Путь	Путь, который требуется добавить в запрос к URL-адресу, указанному в поле **URL** на вкладке **Основные параметры**. Например, если вы укажете путь `/input`, а в качестве URL-адреса укажете `10.10.10.10`, от точки назначения будут исходить запросы `10.10.10.10/input`.
Ожидание проверки работоспособности	Интервал в секундах для проверки работоспособности точки назначения.
Путь проверки работоспособности	URL-адрес для отправки запросов для получения данных о работоспособности системы, с которой ресурс точки назначения устанавливает связь.
Проверка работоспособности	Переключатель, включающий проверку работоспособности. По умолчанию этот переключатель выключен.
Дисковый буфер	Переключатель, включающий использование дискового буфера. По умолчанию этот переключатель включен. Дисковый буфер используется, если коллектор не может отправить в точку назначения нормализованные события. Вы можете указать размер дискового буфера в поле **Размер дискового буфера**. Если в дисковом буфере не останется свободного пространства, новые нормализованные события будут перезаписывать старые нормализованные события, начиная с самого старого.
Время ожидания	Время в секундах, в течение которого точка назначения ожидает ответа другого сервиса или компонента.
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.

Параметр	Описание
Фильтр	Фильтр для определения событий, которые будут обрабатываться ресурсом. Вы можете выбрать существующий фильтр или создать новый фильтр. Для создания нового фильтра выберите значение **Создать**. Если вы хотите изменить параметры существующего фильтра, нажмите рядом с ним на значок карандаша. **Как создать фильтр?** Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. Выберите режим создания фильтра: **Конструктор** или **Код**. При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра. 5. Если вы выбрали вариант **Конструктор**, выполните следующие действия: a. В раскрывающемся списке выберите логический оператор: • **И** – отбирает события, которые соответствуют всем указанным условиям. • **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий. • **НЕ** – отбирает события, которые не соответствуют всем указанным условиям. b. Нажмите на кнопку **Добавить условие**. c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра. **Операнды фильтров** • **Поля событий** – поле события, которое требуется использовать как операнд фильтра. • **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**. Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра. • **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – словарь, который требуется использовать. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря. • **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события. • **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать. • **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы. • **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда. • **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда. • **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.

Параметр	Описание

	• **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
	  • **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
	  • **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
	  • **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
	• **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константа, которую требуется присвоить операнду.
	• **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
	Операторы фильтров
	• **=** – левый операнд равен правому операнду.
	• **<** – левый операнд меньше правого операнда.
	• **<=** – левый операнд меньше или равен правому операнду.
	• **>** – левый операнд больше правого операнда.
	• **>=** – левый операнд больше или равен правому операнду.
	• **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
	• **contains** – левый операнд содержит значения правого операнда.
	• **startsWith** – левый операнд начинается с одного из значений правого операнда.
	• **endsWith** – левый операнд заканчивается одним из значений правого операнда.
	• **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
	• **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).
	Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.
	Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
	• **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
	Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
	• **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
	• **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
	• **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
	• **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
	• **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись.
	• **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.
	Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.
	Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.
	e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.
	Вы можете добавить несколько групп условий.
	6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.
	В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

Параметр	Описание
	7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕. 8. Нажмите **Сохранить**.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису** → **Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип diode

Точки назначения с типом **diode** используются для передачи событий с помощью диода данных. Доступные параметры точки назначения с типом **diode** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Состояние	Переключатель, включающий отправку событий в точку назначения. По умолчанию этот переключатель включен.
Тип	Тип точки назначения – **diode**. Обязательный параметр.

Параметр	Описание
Директория, из которой диод данных получает события	Путь к директории, из которой диод данных перемещает события. Максимальная длина пути составляет до 255 символов в кодировке Unicode. **Ограничения при использовании префиксов к путям на серверах Windows** На серверах Windows необходимо указывать абсолютные пути к директориям. Невозможно использовать директории, названия которых соответствуют указанным ниже регулярным выражениям: • `^[a-zA-Z]:\\Program Files` • `^[a-zA-Z]:\\Program Files \(x86\)` • `^[a-zA-Z]:\\Windows` • `^[a-zA-Z]:\\ProgramData\\Kaspersky Lab\\KUMA` Эти шаблоны используются системой для проверки пути. В них двойные обратные косые черты (\\) используются в качестве части синтаксиса регулярного выражения и не должны указываться в самом пути вручную. **Ограничения при использовании префиксов к путям на серверах Linux** Префиксы, которые невозможно использовать при указании путей к файлам: • `/*` • `/bin` • `/boot` • `/dev` • `/etc` • `/home` • `/lib` • `/lib64` • `/proc` • `/root` • `/run` • `/sys` • `/tmp` • `/usr/*` • `/usr/bin/` • `/usr/local/*` • `/usr/local/sbin/` • `/usr/local/bin/` • `/usr/sbin/` • `/usr/lib/` • `/usr/lib64/` • `/var/*` • `/var/lib/` • `/var/run/` • `/opt/kaspersky/kuma/` Приведенные префиксы используются системой в качестве регулярных выражений для проверки пути. Символ * в префиксах соответствует любой последовательности символов и не должен указываться в самом пути вручную, если это не часть допустимого пути.

Параметр	Описание
	Файлы по указанным ниже путям доступны: • `/opt/kaspersky/kuma/clickhouse/logs/` • `/opt/kaspersky/kuma/metrics/log/` Пути, указанные в полях **Директория, из которой диод данных получает события** и **Временная директория**, не должны совпадать.
Временная директория	Путь к директории, в которой события готовятся для передачи диоду данных. Максимальная длина пути составляет до 255 символов в кодировке Unicode. События собираются в файл по истечении времени ожидания или при переполнении буфера. По умолчанию время ожидания составляет 10 секунд. Подготовленный файл с событиями перемещается в директорию, указанную в поле **Директория, из которой диод данных получает события**. В качестве названия файла с событиями используется хеш-сумма (SHA-256) содержимого файла с событиями. Пути, указанные в полях **Директория, из которой диод данных получает события** и **Временная директория**, не должны совпадать.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Интервал очистки буфера	Интервал в секундах для отправки событий в точку назначения. Значение по умолчанию: 1 секунда.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Сжатие	Определяет, будет ли поток событий, отправляемый агентом Kaspersky SIEM Cloud в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
Разделитель	Символ, определяющий границу между событиями: • **\n**; • **\t**; • **\0**. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений.
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.

Параметр	Описание
Фильтр	Фильтр для определения событий, которые будут обрабатываться ресурсом. Вы можете выбрать существующий фильтр или создать новый фильтр. Для создания нового фильтра выберите значение **Создать**. Если вы хотите изменить параметры существующего фильтра, нажмите рядом с ним на значок карандаша. **Как создать фильтр?** Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. Выберите режим создания фильтра: **Конструктор** или **Код**. При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра. 5. Если вы выбрали вариант **Конструктор**, выполните следующие действия: a. В раскрывающемся списке выберите логический оператор: • **И** – отбирает события, которые соответствуют всем указанным условиям. • **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий. • **НЕ** – отбирает события, которые не соответствуют всем указанным условиям. b. Нажмите на кнопку **Добавить условие**. c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра. **Операнды фильтров** • **Поля событий** – поле события, которое требуется использовать как операнд фильтра. • **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **`Ctrl`**/**`Command`**+**`F1`**. Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра. • **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – словарь, который требуется использовать. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря. • **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события. • **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать. • **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы. • **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда. • **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда. • **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.

Параметр	Описание

	• **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
	  • **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
	  • **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
	  • **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
	• **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константа, которую требуется присвоить операнду.
	• **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
	Операторы фильтров
	• **=** – левый операнд равен правому операнду.
	• **<** – левый операнд меньше правого операнда.
	• **<=** – левый операнд меньше или равен правому операнду.
	• **>** – левый операнд больше правого операнда.
	• **>=** – левый операнд больше или равен правому операнду.
	• **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
	• **contains** – левый операнд содержит значения правого операнда.
	• **startsWith** – левый операнд начинается с одного из значений правого операнда.
	• **endsWith** – левый операнд заканчивается одним из значений правого операнда.
	• **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
	• **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).
	Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.
	Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
	• **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
	Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
	• **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
	• **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
	• **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
	• **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
	• **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись.
	• **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.
	Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.
	Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.
	e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.
	Вы можете добавить несколько групп условий.
	6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.
	В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

Параметр	Описание
	7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕. 8. Нажмите **Сохранить**.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису → Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип kafka

Точки назначения с типом **kafka** используются для коммуникаций с помощью kafka. Доступные параметры точки назначения с типом **kafka** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Состояние	Переключатель, включающий отправку событий в точку назначения. По умолчанию этот переключатель включен.
Тип	Тип точки назначения – **kafka**. Обязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Поддерживаются следующие форматы URL-адресов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address><port number>`. IPv6-адреса можно указать в формате `[<IPv6 address>%<interface>:<port number>`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Вы можете добавить несколько URL-адресов и удалить URL-адрес. Kaspersky SIEM Cloud не позволяет сохранить ресурс или сервис если в поле URL есть знак табуляции или пробел. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр.
Топик	Тема сообщений Kafka. Максимальная длина темы составляет до 255 символов. Вы можете использовать следующие символы: a–z, A–Z, 0–9, ".", "_", "-". Обязательный параметр.

Параметр	Описание
Авторизация	Тип авторизации при подключении к URL-адресу, указанному в поле **URL**. • **Выключена**. Это значение выбрано по умолчанию. • **Обычная**. Этот тип авторизации осуществляется с помощью механизма SASL/PLAIN, который передает имя пользователя и пароль в открытом виде. Как правило, для обеспечения безопасности передачи данных (шифрования) в SASL/PLAIN используется TLS. При выборе этого значения в раскрывающемся списке **Секрет** укажите секрет, содержащий учетные данные пользователя для авторизации при подключении к точке назначения. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать секрет?** *Чтобы создать секрет:* 1. В поле **Название** введите название секрета. 2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору. 3. При необходимости в поле **Описание** введите описание секрета. 4. Нажмите на кнопку **Создать**. Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**. • **PFX** – использовать шифрование TLS с PFX-секретом. Вам нужно сформировать PFX-сертификат с закрытым ключом в формате PKCS#12-контейнера во внешнем центре сертификации, экспортировать PFX-сертификат из хранилища, после чего загрузить PFX-сертификат в веб-интерфейс Kaspersky SIEM Cloud в виде PFX-секрета. При выборе этого значения в раскрывающемся списке **PFX секрет** укажите PFX-секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий PFX-секрет или создать новый PFX-секрет. Для создания нового PFX-секрета выберите значение **Создать**. Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша. **Как создать PFX-секрет?** *Чтобы создать PFX-секрет:* 1. В поле **Название** введите название PFX-секрета. 2. Нажмите на кнопку **Загрузить PFX** и выберите файл в формате PKCS#12-контейнера, в который вы экспортировали файл PFX с закрытым ключом. 3. В поле **Пароль** введите пароль для защиты файла PFX, указанный в мастере экспорта PFX. 4. Нажмите на кнопку **Создать**. PFX-секрет будет создан и отобразится в раскрывающемся списке **PFX секрет**.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Интервал очистки буфера	Интервал в секундах для отправки событий в точку назначения. Значение по умолчанию: 1 секунда.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию: 10 ГБ, в интерфейсе отображается как 0.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.

Параметр	Описание
Выходной формат	Формат, в котором события отправляются во внешний источник: • **JSON**. • **CEF**. При выборе этого значения в отправляемых событиях содержится заголовок CEF и только поля с непустыми значениями. • **Syslog-CEF**.

Режим TLS	Режим шифрования TLS. При использовании шифрования TLS вы не можете указать IP-адрес в поле **URL** на вкладке **Основные параметры**. Доступные значения:
	• **Выключено** – не использовать шифрование TLS. Это значение выбрано по умолчанию.
	• **Включено** – использовать шифрование TLS, но без верификации сертификатов.
	• **Нестандартный CA** – использовать шифрование TLS с верификацией сертификата, подписанного центром сертификации. При выборе этого значения в раскрывающемся списке **Нестандартный CA** укажите секрет с сертификатом, подписанным центром сертификации. Вы можете выбрать существующий секрет или создать новый секрет. Для создания нового секрета выберите значение **Создать**.
	Если вы хотите изменить параметры существующего секрета, нажмите рядом с ним на значок карандаша.
	Как создать сертификат, подписанный центром сертификации?
	Вы можете создать сертификат, подписанный центром сертификации, на сервере Ядра Kaspersky SIEM Cloud (в примерах команд ниже используется OpenSSL).
	Чтобы создать сертификат, подписанный центром сертификации:
	1. Создайте ключ, который будет использоваться центром сертификации, например:
	`openssl genrsa -out ca.key 2048`
	2. Создайте сертификат для созданного ключа, например:
	`openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<common name of the certification authority host>" -out ca.crt`
	3. Создайте приватный ключ и запрос на его подписание в центре сертификации, например:
	`openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=<common host name of the Kaspersky SIEM Cloud server>" -out server.csr`
	4. Создайте сертификат, подписанный центром сертификации. Вам нужно включить в переменную `subjectAltName` доменные имена или IP-адреса сервера, для которого вы создаете сертификат, например:
	`openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`
	5. Загрузите созданный сертификат `server.crt` в веб-интерфейсе Kaspersky SIEM Cloud в секрет с типом **certificate**, после чего в раскрывающемся списке **Нестандартный CA** выберите секрет с типом **certificate**.
	Для использования сертификатов Kaspersky SIEM Cloud на сторонних устройствах вам нужно изменить расширение файла сертификата с CERT на CRT. В противном случае вы можете получить ошибку `x509: certificate signed by unknown authority`.

Сжатие	Определяет, будет ли поток событий, отправляемый агентом Kaspersky SIEM Cloud в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**. • **LZ4**. • **zstd**. Если вы не выберете значение, сжатие будет выключено (значение по умолчанию).
Разделитель	Символ, определяющий границу между событиями: • **\n**; • **\t**; • **\0**. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений.
Дисковый буфер	Переключатель, включающий использование дискового буфера. По умолчанию этот переключатель включен. Дисковый буфер используется, если коллектор не может отправить в точку назначения нормализованные события. Вы можете указать размер дискового буфера в поле **Размер дискового буфера**. Если в дисковом буфере не останется свободного пространства, новые нормализованные события будут перезаписывать старые нормализованные события, начиная с самого старого.
Время ожидания	Время в секундах, в течение которого точка назначения ожидает ответа другого сервиса или компонента.

Параметр	Описание
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.

Параметр	Описание
Фильтр	Фильтр для определения событий, которые будут обрабатываться ресурсом. Вы можете выбрать существующий фильтр или создать новый фильтр. Для создания нового фильтра выберите значение **Создать**. Если вы хотите изменить параметры существующего фильтра, нажмите рядом с ним на значок карандаша. **Как создать фильтр?** Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. Выберите режим создания фильтра: **Конструктор** или **Код**. При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра. 5. Если вы выбрали вариант **Конструктор**, выполните следующие действия: a. В раскрывающемся списке выберите логический оператор: • **И** – отбирает события, которые соответствуют всем указанным условиям. • **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий. • **НЕ** – отбирает события, которые не соответствуют всем указанным условиям. b. Нажмите на кнопку **Добавить условие**. c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра. **Операнды фильтров** • **Поля событий** – поле события, которое требуется использовать как операнд фильтра. • **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**. Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра. • **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – словарь, который требуется использовать. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря. • **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события. • **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать. • **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы. • **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда. • **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда. • **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.

Параметр	Описание

	• **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
	  • **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
	  • **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
	  • **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
	• **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константа, которую требуется присвоить операнду.
	• **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
	Операторы фильтров
	• **=** – левый операнд равен правому операнду.
	• **<** – левый операнд меньше правого операнда.
	• **<=** – левый операнд меньше или равен правому операнду.
	• **>** – левый операнд больше правого операнда.
	• **>=** – левый операнд больше или равен правому операнду.
	• **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
	• **contains** – левый операнд содержит значения правого операнда.
	• **startsWith** – левый операнд начинается с одного из значений правого операнда.
	• **endsWith** – левый операнд заканчивается одним из значений правого операнда.
	• **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
	• **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).
	Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.
	Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
	• **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
	Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
	• **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
	• **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
	• **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
	• **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
	• **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в коррелляторах.
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись.
	• **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.
	Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.
	Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.
	e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.
	Вы можете добавить несколько групп условий.
	6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.
	В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

Параметр	Описание
	7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕. 8. Нажмите **Сохранить**.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису** → **Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип file

Точки назначения с типом **file** используются для записи в файл. Доступные параметры точки назначения с типом **file** описаны в таблицах ниже.

При удалении точки назначения с типом **file**, используемой в сервисе, вам нужно перезапустить сервис.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Состояние	Переключатель, включающий отправку событий в точку назначения. По умолчанию этот переключатель включен.
Тип	Тип точки назначения – **file**. Обязательный параметр.

Параметр	Описание
URL	Путь к файлу, в который требуется записать события. **Ограничения при использовании префиксов к путям файлов** Префиксы, которые невозможно использовать при указании путей к файлам: • `/*` • `/bin` • `/boot` • `/dev` • `/etc` • `/home` • `/lib` • `/lib64` • `/proc` • `/root` • `/run` • `/sys` • `/tmp` • `/usr/*` • `/usr/bin/` • `/usr/local/*` • `/usr/local/sbin/` • `/usr/local/bin/` • `/usr/sbin/` • `/usr/lib/` • `/usr/lib64/` • `/var/*` • `/var/lib/` • `/var/run/` • `/opt/kaspersky/kuma/` Приведенные префиксы используются системой в качестве регулярных выражений для проверки пути. Символ * в префиксах соответствует любой последовательности символов и не должен указываться в самом пути вручную, если это не часть допустимого пути. Файлы по указанным ниже путям доступны: • `/opt/kaspersky/kuma/clickhouse/logs/` • `/opt/kaspersky/kuma/metrics/log/` Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Интервал очистки буфера	Интервал в секундах для отправки событий в точку назначения. Значение по умолчанию: 1 секунда.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию: 10 ГБ, в интерфейсе отображается как 0.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Выходной формат	Формат, в котором события отправляются во внешний источник: • **JSON**. • **CEF**. При выборе этого значения в отправляемых событиях содержится заголовок CEF и только поля с непустыми значениями. • **Syslog-CEF**.
Разделитель	Символ, определяющий границу между событиями: • **\n**; • **\t**; • **\0**. Если вы не выберете значение в этом раскрывающемся списке, по умолчанию будет выбрано пустое значение. В этом случае коннектор не будет разделять одно событие на несколько и передаст его в нормализатор без изменений.
Дисковый буфер	Переключатель, включающий использование дискового буфера. По умолчанию этот переключатель включен. Дисковый буфер используется, если коллектор не может отправить в точку назначения нормализованные события. Вы можете указать размер дискового буфера в поле **Размер дискового буфера**. Если в дисковом буфере не останется свободного пространства, новые нормализованные события будут перезаписывать старые нормализованные события, начиная с самого старого.
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.

Параметр	Описание
Фильтр	Фильтр для определения событий, которые будут обрабатываться ресурсом. Вы можете выбрать существующий фильтр или создать новый фильтр. Для создания нового фильтра выберите значение **Создать**. Если вы хотите изменить параметры существующего фильтра, нажмите рядом с ним на значок карандаша. **Как создать фильтр?** Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. Выберите режим создания фильтра: **Конструктор** или **Код**. При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра. 5. Если вы выбрали вариант **Конструктор**, выполните следующие действия: a. В раскрывающемся списке выберите логический оператор: • **И** – отбирает события, которые соответствуют всем указанным условиям. • **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий. • **НЕ** – отбирает события, которые не соответствуют всем указанным условиям. b. Нажмите на кнопку **Добавить условие**. c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра. **Операнды фильтров** • **Поля событий** – поле события, которое требуется использовать как операнд фильтра. • **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**. Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра. • **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – словарь, который требуется использовать. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря. • **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события. • **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать. • **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы. • **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда. • **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда. • **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.

Параметр	Описание

	• **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
	  • **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
	  • **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
	  • **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
	• **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константа, которую требуется присвоить операнду.
	• **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
	Операторы фильтров
	• **=** – левый операнд равен правому операнду.
	• **<** – левый операнд меньше правого операнда.
	• **<=** – левый операнд меньше или равен правому операнду.
	• **>** – левый операнд больше правого операнда.
	• **>=** – левый операнд больше или равен правому операнду.
	• **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
	• **contains** – левый операнд содержит значения правого операнда.
	• **startsWith** – левый операнд начинается с одного из значений правого операнда.
	• **endsWith** – левый операнд заканчивается одним из значений правого операнда.
	• **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
	• **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).
	Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.
	Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
	• **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
	Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
	• **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
	• **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
	• **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
	• **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
	• **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись.
	• **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.
	Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.
	Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.
	e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.
	Вы можете добавить несколько групп условий.
	6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.
	В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

Параметр	Описание
	7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕. 8. Нажмите **Сохранить**.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису → Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип storage

Точки назначения с типом **storage** используются для передачи данных в хранилище. Доступные параметры точки назначения с типом **storage** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Состояние	Переключатель, включающий отправку событий в точку назначения. По умолчанию этот переключатель включен.
Тип	Тип точки назначения – **storage**. Обязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Поддерживаются следующие форматы URL-адресов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address><port number>`. IPv6-адреса можно указать в формате `[<IPv6 address>%<interface>:<port number>`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Вы можете добавить несколько URL-адресов и удалить URL-адрес. Kaspersky SIEM Cloud не позволяет сохранить ресурс или сервис если в поле URL есть знак табуляции или пробел. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Интервал очистки буфера	Интервал в секундах для отправки событий в точку назначения. Значение по умолчанию: 1 секунда.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию: 10 ГБ, в интерфейсе отображается как 0.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Прокси-сервер	Прокси-сервер для точки назначения. Вы можете выбрать существующий прокси-сервер или создать новый прокси-сервер. Для создания нового прокси-сервера выберите **Создать**. Если вы хотите изменить параметры существующего прокси-сервера, нажмите рядом с ним на значок карандаша .
Сжатие	Определяет, будет ли поток событий, отправляемый агентом Kaspersky SIEM Cloud в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
Политика выбора URL	Способ определения URL-адресов, на которые события отправляются в первую очередь, если вы добавили несколько URL-адресов в поле **URL** на вкладке **Основные параметры**: • **Любой** – события отправляются на случайно выбранный доступный URL-адрес до тех пор, пока URL-адрес принимает события. Если URL-адрес станет недоступным, события будут отправляться на другой случайно выбранный доступный URL-адрес. Это значение выбрано по умолчанию. • **Сначала первый** – события отправляются на первый добавленный URL-адрес. Если URL-адрес станет недоступным, события будут отправляться на следующий добавленный доступный URL-адрес. Если первый добавленный URL-адрес снова станет доступным, события будут отправляться на него. • **Сбалансированный** – события равномерно распределяются между доступными URL-адресами. Этот способ определения URL-адресов не гарантирует равномерного распределения событий по URL-адресам, так как буфер может быть переполнен или события могут быть отправлены в точку назначения. Вы можете указать размер буфера в байтах в поле **Размер буфера**, а также указать интервал в секундах для отправки событий в точку назначения в поле **Интервал очистки буфера**.
Ожидание проверки работоспособности	Интервал в секундах для проверки работоспособности точки назначения.
Дисковый буфер	Переключатель, включающий использование дискового буфера. По умолчанию этот переключатель включен. Дисковый буфер используется, если коллектор не может отправить в точку назначения нормализованные события. Вы можете указать размер дискового буфера в поле **Размер дискового буфера**. Если в дисковом буфере не останется свободного пространства, новые нормализованные события будут перезаписывать старые нормализованные события, начиная с самого старого.
Время ожидания	Время в секундах, в течение которого точка назначения ожидает ответа другого сервиса или компонента.
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.

Параметр	Описание
Фильтр	Фильтр для определения событий, которые будут обрабатываться ресурсом. Вы можете выбрать существующий фильтр или создать новый фильтр. Для создания нового фильтра выберите значение **Создать**. Если вы хотите изменить параметры существующего фильтра, нажмите рядом с ним на значок карандаша. **Как создать фильтр?** Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. Выберите режим создания фильтра: **Конструктор** или **Код**. При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра. 5. Если вы выбрали вариант **Конструктор**, выполните следующие действия: a. В раскрывающемся списке выберите логический оператор: • **И** – отбирает события, которые соответствуют всем указанным условиям. • **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий. • **НЕ** – отбирает события, которые не соответствуют всем указанным условиям. b. Нажмите на кнопку **Добавить условие**. c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра. **Операнды фильтров** • **Поля событий** – поле события, которое требуется использовать как операнд фильтра. • **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**. Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра. • **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – словарь, который требуется использовать. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря. • **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события. • **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать. • **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы. • **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда. • **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда. • **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.

Параметр	Описание

	• **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
	  • **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
	  • **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
	  • **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
	• **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константа, которую требуется присвоить операнду.
	• **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
	Операторы фильтров
	• **=** – левый операнд равен правому операнду.
	• **<** – левый операнд меньше правого операнда.
	• **<=** – левый операнд меньше или равен правому операнду.
	• **>** – левый операнд больше правого операнда.
	• **>=** – левый операнд больше или равен правому операнду.
	• **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
	• **contains** – левый операнд содержит значения правого операнда.
	• **startsWith** – левый операнд начинается с одного из значений правого операнда.
	• **endsWith** – левый операнд заканчивается одним из значений правого операнда.
	• **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
	• **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).
	Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.
	Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
	• **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
	Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
	• **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
	• **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
	• **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
	• **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
	• **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись.
	• **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.
	Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.
	Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.
	e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.
	Вы можете добавить несколько групп условий.
	6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.
	В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

Параметр	Описание
	7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕. 8. Нажмите **Сохранить**.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису → Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип correlator

Точки назначения с типом **correlator** используются для передачи данных в коррелятор. Доступные параметры точки назначения с типом **correlator** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Состояние	Переключатель, включающий отправку событий в точку назначения. По умолчанию этот переключатель включен.
Тип	Тип точки назначения – **correlator**. Обязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Поддерживаются следующие форматы URL-адресов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address><port number>`. IPv6-адреса можно указать в формате `[<IPv6 address>%<interface>:<port number>`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Вы можете добавить несколько URL-адресов и удалить URL-адрес. Kaspersky SIEM Cloud не позволяет сохранить ресурс или сервис если в поле URL есть знак табуляции или пробел. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Интервал очистки буфера	Интервал в секундах для отправки событий в точку назначения. Значение по умолчанию: 1 секунда.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию: 10 ГБ, в интерфейсе отображается как 0.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Прокси-сервер	Прокси-сервер для точки назначения. Вы можете выбрать существующий прокси-сервер или создать новый прокси-сервер. Для создания нового прокси-сервера выберите **Создать**. Если вы хотите изменить параметры существующего прокси-сервера, нажмите рядом с ним на значок карандаша .
Сжатие	Определяет, будет ли поток событий, отправляемый агентом Kaspersky SIEM Cloud в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
Политика выбора URL	Способ определения URL-адресов, на которые события отправляются в первую очередь, если вы добавили несколько URL-адресов в поле **URL** на вкладке **Основные параметры**: • **Любой** – события отправляются на случайно выбранный доступный URL-адрес до тех пор, пока URL-адрес принимает события. Если URL-адрес станет недоступным, события будут отправляться на другой случайно выбранный доступный URL-адрес. Это значение выбрано по умолчанию. • **Сначала первый** – события отправляются на первый добавленный URL-адрес. Если URL-адрес станет недоступным, события будут отправляться на следующий добавленный доступный URL-адрес. Если первый добавленный URL-адрес снова станет доступным, события будут отправляться на него. • **Сбалансированный** – события равномерно распределяются между доступными URL-адресами. Этот способ определения URL-адресов не гарантирует равномерного распределения событий по URL-адресам, так как буфер может быть переполнен или события могут быть отправлены в точку назначения. Вы можете указать размер буфера в байтах в поле **Размер буфера**, а также указать интервал в секундах для отправки событий в точку назначения в поле **Интервал очистки буфера**.
Ожидание проверки работоспособности	Интервал в секундах для проверки работоспособности точки назначения.
Дисковый буфер	Переключатель, включающий использование дискового буфера. По умолчанию этот переключатель включен. Дисковый буфер используется, если коллектор не может отправить в точку назначения нормализованные события. Вы можете указать размер дискового буфера в поле **Размер дискового буфера**. Если в дисковом буфере не останется свободного пространства, новые нормализованные события будут перезаписывать старые нормализованные события, начиная с самого старого.
Время ожидания	Время в секундах, в течение которого точка назначения ожидает ответа другого сервиса или компонента.
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.

Параметр	Описание
Фильтр	Фильтр для определения событий, которые будут обрабатываться ресурсом. Вы можете выбрать существующий фильтр или создать новый фильтр. Для создания нового фильтра выберите значение **Создать**. Если вы хотите изменить параметры существующего фильтра, нажмите рядом с ним на значок карандаша. **Как создать фильтр?** Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. Выберите режим создания фильтра: **Конструктор** или **Код**. При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра. 5. Если вы выбрали вариант **Конструктор**, выполните следующие действия: a. В раскрывающемся списке выберите логический оператор: • **И** – отбирает события, которые соответствуют всем указанным условиям. • **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий. • **НЕ** – отбирает события, которые не соответствуют всем указанным условиям. b. Нажмите на кнопку **Добавить условие**. c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра. **Операнды фильтров** • **Поля событий** – поле события, которое требуется использовать как операнд фильтра. • **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**. Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра. • **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – словарь, который требуется использовать. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря. • **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события. • **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать. • **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы. • **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда. • **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда. • **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.

Параметр	Описание

	• **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
	  • **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
	  • **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
	  • **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
	• **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константа, которую требуется присвоить операнду.
	• **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
	Операторы фильтров
	• **=** – левый операнд равен правому операнду.
	• **<** – левый операнд меньше правого операнда.
	• **<=** – левый операнд меньше или равен правому операнду.
	• **>** – левый операнд больше правого операнда.
	• **>=** – левый операнд больше или равен правому операнду.
	• **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
	• **contains** – левый операнд содержит значения правого операнда.
	• **startsWith** – левый операнд начинается с одного из значений правого операнда.
	• **endsWith** – левый операнд заканчивается одним из значений правого операнда.
	• **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
	• **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).
	Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.
	Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
	• **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
	Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
	• **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
	• **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
	• **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
	• **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
	• **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись.
	• **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.
	Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.
	Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.
	e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.
	Вы можете добавить несколько групп условий.
	6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.
	В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

Параметр	Описание
	7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕. 8. Нажмите **Сохранить**.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису → Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Точка назначения, тип eventRouter

Точки назначения с типом **eventRouter** используются для передачи событий в маршрутизатор событий. Доступные параметры точки назначения с типом **eventRouter** описаны в таблицах ниже.

Вкладка Основные параметры

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Состояние	Переключатель, включающий отправку событий в точку назначения. По умолчанию этот переключатель включен.
Тип	Тип точки назначения – **eventRouter**. Обязательный параметр.
URL	URL-адрес, с которым требуется установить связь. Поддерживаются следующие форматы URL-адресов: • `<host name>:<port number>`; • `<IPv4 address>:<port number>`; • `<IPv6 address><port number>`. IPv6-адреса можно указать в формате `[<IPv6 address>%<interface>:<port number>`, например `[fe80::5054:ff:fe4d:ba0c%eth0]:4222`. Вы можете добавить несколько URL-адресов и удалить URL-адрес. Kaspersky SIEM Cloud не позволяет сохранить ресурс или сервис если в поле URL есть знак табуляции или пробел. Для добавления URL-адреса нажмите на кнопку **+ Добавить**. Для удаления URL-адреса нажмите рядом с ним на значок удаления ✕. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.

Вкладка Дополнительные параметры

Параметр	Описание
Размер буфера	Размер буфера в байтах для накопления событий в оперативной памяти сервера перед отправкой на дальнейшую обработку или хранение. Вы можете указать целое положительное число. Размер буфера по умолчанию: 67 108 864 (64 МБ), в интерфейсе отображается как 0.
Интервал очистки буфера	Интервал в секундах для отправки событий в точку назначения. Значение по умолчанию: 1 секунда.
Размер дискового буфера	Размер дискового буфера в байтах. Значение по умолчанию: 10 ГБ, в интерфейсе отображается как 0.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Допускается указать целое положительное число не больше 999.
Прокси-сервер	Прокси-сервер для точки назначения. Вы можете выбрать существующий прокси-сервер или создать новый прокси-сервер. Для создания нового прокси-сервера выберите **Создать**. Если вы хотите изменить параметры существующего прокси-сервера, нажмите рядом с ним на значок карандаша .
Сжатие	Определяет, будет ли поток событий, отправляемый агентом Kaspersky SIEM Cloud в точку назначения, сжиматься перед передачей. Доступные значения: • **Выключено**. • **Snappy**. • **gzip**.
Политика выбора URL	Способ определения URL-адресов, на которые события отправляются в первую очередь, если вы добавили несколько URL-адресов в поле **URL** на вкладке **Основные параметры**: • **Любой** – события отправляются на случайно выбранный доступный URL-адрес до тех пор, пока URL-адрес принимает события. Если URL-адрес станет недоступным, события будут отправляться на другой случайно выбранный доступный URL-адрес. Это значение выбрано по умолчанию. • **Сначала первый** – события отправляются на первый добавленный URL-адрес. Если URL-адрес станет недоступным, события будут отправляться на следующий добавленный доступный URL-адрес. Если первый добавленный URL-адрес снова станет доступным, события будут отправляться на него. • **Сбалансированный** – события равномерно распределяются между доступными URL-адресами. Этот способ определения URL-адресов не гарантирует равномерного распределения событий по URL-адресам, так как буфер может быть переполнен или события могут быть отправлены в точку назначения. Вы можете указать размер буфера в байтах в поле **Размер буфера**, а также указать интервал в секундах для отправки событий в точку назначения в поле **Интервал очистки буфера**.
Ожидание проверки работоспособности	Интервал в секундах для проверки работоспособности точки назначения.
Дисковый буфер	Переключатель, включающий использование дискового буфера. По умолчанию этот переключатель включен. Дисковый буфер используется, если коллектор не может отправить в точку назначения нормализованные события. Вы можете указать размер дискового буфера в поле **Размер дискового буфера**. Если в дисковом буфере не останется свободного пространства, новые нормализованные события будут перезаписывать старые нормализованные события, начиная с самого старого.
Время ожидания	Время в секундах, в течение которого точка назначения ожидает ответа другого сервиса или компонента.
Отладка	Переключатель, включающий логирование ресурса. По умолчанию переключатель выключен.

Параметр	Описание
Фильтр	Фильтр для определения событий, которые будут обрабатываться ресурсом. Вы можете выбрать существующий фильтр или создать новый фильтр. Для создания нового фильтра выберите значение **Создать**. Если вы хотите изменить параметры существующего фильтра, нажмите рядом с ним на значок карандаша. **Как создать фильтр?** Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. Выберите режим создания фильтра: **Конструктор** или **Код**. При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра. 5. Если вы выбрали вариант **Конструктор**, выполните следующие действия: a. В раскрывающемся списке выберите логический оператор: • **И** – отбирает события, которые соответствуют всем указанным условиям. • **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий. • **НЕ** – отбирает события, которые не соответствуют всем указанным условиям. b. Нажмите на кнопку **Добавить условие**. c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра. **Операнды фильтров** • **Поля событий** – поле события, которое требуется использовать как операнд фильтра. • **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**. Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра. • **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – словарь, который требуется использовать. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря. • **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события. • **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать. • **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы. • **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда. • **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда. • **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.

Параметр	Описание

	• **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
	  • **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
	  • **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
	  • **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
	• **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константа, которую требуется присвоить операнду.
	• **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
	Операторы фильтров
	• **=** – левый операнд равен правому операнду.
	• **<** – левый операнд меньше правого операнда.
	• **<=** – левый операнд меньше или равен правому операнду.
	• **>** – левый операнд больше правого операнда.
	• **>=** – левый операнд больше или равен правому операнду.
	• **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
	• **contains** – левый операнд содержит значения правого операнда.
	• **startsWith** – левый операнд начинается с одного из значений правого операнда.
	• **endsWith** – левый операнд заканчивается одним из значений правого операнда.
	• **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
	• **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).
	Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.
	Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
	• **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
	Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
	• **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
	• **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
	• **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
	• **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
	• **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись.
	• **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.
	Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.
	Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.
	e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.
	Вы можете добавить несколько групп условий.
	6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.
	В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

Параметр	Описание
	7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕. 8. Нажмите **Сохранить**.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров точки назначения и используется для привязки к коллекторам, корреляторам и маршрутизаторам событий.

Для привязки точки назначения к сервису, нажмите на кнопку **Привязать к сервису** → **Привязать к <название_сервиса>**. В открывшемся окне выберите один или несколько сервисов и нажмите **OK**. Точка назначения будет привязана к выбранным сервисам.

При необходимости вы можете отвязать точку назначения от сервиса. Для этого нужно установить флажок рядом с нужным сервисом, нажать **Удалить** и подтвердить удаление привязки к сервису.

Использование прокси-сервера

Прокси-серверы используются для хранения параметров конфигурации прокси-серверов, например в точках назначения. Поддерживается тип http.

Чтобы создать прокси-сервер:

1. В веб-интерфейсе перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Прокси-серверы** и нажмите кнопку **Создать**.

2. В поле **Название** укажите уникальное имя прокси-сервера. Максимальная длина имени: от 128 символов в кодировке Unicode.

3. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит прокси-сервер.

4. Настройте параметры подключения к прокси-серверу, выполнив следующие действия:

   - Если нужно хранить URL прокси-сервера и учетные данные отдельно, установите флажок **Секрет отдельно** и заполните следующие поля:

     a. В поле **URL** укажите URL-адрес прокси-сервера.

     b. В раскрывающемся списке **Секрет** выберите секрет или создайте новый с типом **credentials**, нажав кнопку **Создать**.

     Как создать секрет?

     Чтобы создать секрет:

     1. В поле **Название** введите название секрета.

     2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору.

3. При необходимости в поле **Описание** введите описание секрета.

4. Нажмите на кнопку **Создать**.

   Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**.

Если флажок **Секрет отдельно** установлен, информация о подключении к прокси-серверу отображается в интерфейсе, поэтому при изменении пароля достаточно обновить секрет без пересоздания подключений. По умолчанию флажок снят.

- Если вы хотите хранить URL прокси-сервера в секрете, в раскрывающемся списке **Брать URL из секрета** выберите ресурс секрета.

  Вы можете создать и изменить секрет. Для создания секрета нажмите кнопку **Создать**, а для изменения секрета нажмите на значок карандаша ( ).

  > Мы не рекомендуем использовать этот параметр. Вместо этого указывайте URL и секрет отдельно вручную, установив флажок **Секрет отдельно**.

5. В раскрывающемся списке **Не использовать на доменах** выберите домены, на которых не должен использоваться прокси-сервер.

6. При необходимости в поле **Описание** введите описание прокси-сервера. Максимальная длина описания: до 4000 символов в кодировке Unicode.

7. Нажмите кнопку **Создать**.

Использование словаря

Словари – это ресурсы, в которых хранятся данные, которые могут использоваться другими ресурсами и сервисами Kaspersky SIEM.

В поставку Kaspersky SIEM Cloud включены предустановленные словари, которые вы также можете использовать при создании правила корреляции, нормализатора, правила обогащения и фильтра.

Предустановленные словари

Предустановленные словари

Название словаря	Тип	Описание
[OOTB] Ahnlab. Severity	dictionary	Содержит таблицу соответствия между идентификатором приоритета и его названием.
[OOTB] Ahnlab. SeverityOperational	dictionary	Содержит значения параметра SeverityOperational и соответствующее ему описание.
[OOTB] Ahnlab. VendorAction	dictionary	Содержит таблицу соответствия между идентификатором выполняемой операции и ее названием.
[OOTB] Cisco ISE Message Codes	dictionary	Содержит коды событий Cisco ISE и соответствующие им имена.
[OOTB] DNS. Opcodes	dictionary	Содержит таблицу соответствия между десятичными кодами операций DNS и их описаниями, зарегистрированными IANA.
[OOTB] IANAProtocolNumbers	dictionary	Содержит номера портов транспортных протоколов (TCP, UDP) и соответствующие им имена сервисов, зарегистрированные IANA.
[OOTB] Juniper - JUNOS	dictionary	Содержит идентификаторы событий JUNOS и соответствующие им описания.
[OOTB] KEDR. AccountType	dictionary	Содержит идентификатор типа учетной записи и соответствующее ему наименование типа.

[OOTB] KEDR. FileAttributes	dictionary	Содержит идентификаторы атрибутов файлов, хранимые файловой системой, и соответствующие им описания.
[OOTB] KEDR. FileOperationType	dictionary	Содержит идентификаторы операций с файлами из API KATA и соответствующие им названия операции.
[OOTB] KEDR. FileType	dictionary	Содержит идентификаторы измененного файла из API KATA и соответствующие им описания типов файлов.
[OOTB] KEDR. IntegrityLevel	dictionary	Содержит SID параметра INTEGRITY LEVEL операционной системы Microsoft Windows и соответствующие им описания.
[OOTB] KEDR. RegistryOperationType	dictionary	Содержит идентификаторы операций с реестром из API KATA и соответствующие им значения.
[OOTB] Linux. Sycall types	dictionary	Содержит идентификаторы системных вызовов ОС Linux и соответствующие им названия.
[OOTB] MariaDB Error Codes	dictionary	Словарь содержит коды ошибок СУБД MariaDB и используется нормализатором [OOTB] MariaDB Audit Plugin syslog для обогащения событий.
[OOTB] Microsoft SQL Server codes	dictionary	Содержит идентификаторы ошибок MS SQL Server и соответствующие им описания.
[OOTB] MS DHCP Event IDs Description	dictionary	Содержит идентификаторы событий DHCP сервера Microsoft Windows и соответствующие им описания.
[OOTB] S-Terra. Dictionary MSG ID to Name	dictionary	Содержит идентификаторы событий устройств S-Terra и соответствующие им имена событий.
[OOTB] S-Terra. MSG_ID to Severity	dictionary	Содержит идентификаторы событий устройств S-Terra и соответствующие им значения Severity.
[OOTB] Syslog Priority To Facility and Severity	table	Таблица содержит значения **Priority** и соответствующие ему значения полей **Facility and Severity**.
[OOTB] VipNet Coordinator Syslog Direction	dictionary	Содержит идентификаторы направления (последовательность специальных символов), используемые в ViPNet Coordinator для обозначения направления, и соответствующие им значения.
[OOTB] Wallix EventClassId - DeviceAction	dictionary	Содержит идентификаторы событий Wallix AdminBastion и соответствующие им описания.
[OOTB] Windows.Codes (4738)	dictionary	Содержит коды операции, присутствующие в событии аудита MS Windows с идентификатором 4738, и соответствующие им имена.
[OOTB] Windows.Codes (4719)	dictionary	Содержит коды операции, присутствующие в событии аудита MS Windows с идентификатором 4719, и соответствующие им имена.
[OOTB] Windows.Codes (4663)	dictionary	Содержит коды операции, присутствующие в событии аудита MS Windows с идентификатором 4663, и соответствующие им имена.
[OOTB] Windows.Codes (4662)	dictionary	Содержит коды операции, присутствующие в событии аудита MS Windows с идентификатором 4662, и соответствующие им имена.
[OOTB] Windows. EventIDs and Event Names mapping	dictionary	Содержит идентификаторы событий ОС Windows и соответствующие имена событий.
[OOTB] Windows. FailureCodes (4625)	dictionary	Содержит идентификаторы из полей **Failure Information\Status** и **Failure Information\Sub Status** события 4625 Microsoft Windows и соответствующие им описания.
[OOTB] Windows. ImpersonationLevels (4624)	dictionary	Содержит идентификаторы из поля **Impersonation level** событий с идентификатором 4624 Microsoft Windows и соответствующие им описания.
[OOTB] Windows. KRB ResultCodes	dictionary	Содержит коды ошибок Kerberos v5 и соответствующие им описания.
[OOTB] Windows. LogonTypes (Windows all events)	dictionary	Содержит идентификаторы типов входов пользователя и соответствующие им наименования.
[OOTB] Windows_Terminal Server. EventIDs and Event Names mapping	dictionary	Содержит идентификаторы событий Microsoft Terminal Server и соответствующие им имена.
[OOTB] Windows. Validate Cred. Error Codes	dictionary	Содержит идентификаторы типов входов пользователя и соответствующие им наименования.
[OOTB] ViPNet Coordinator Syslog Direction	dictionary	Содержит идентификаторы направления (последовательность специальных символов), используемые в ViPNet Coordinator для обозначения направления и соответствующие им значения.
[OOTB] Syslog Priority To Facility and Severity	table	Содержит значения Priority и соответствующие ему значения полей Facility and Severity.

[OOTB] Continent 3.9. Server Access Log Event Type	dictionary	Словарь содержит идентификаторы событий Server Access Log и соответствующие им описания.
[OOTB] Event Categorization table	table	Таблица, содержащая данные для категоризации событий.
[OOTB] FTP. Commands descriptions	dictionary	Словарь содержит команды FTP сервера и соответствующие им описания.
[OOTB] FTP. Server codes	dictionary	Словарь содержит коды FTP сервера и соответствующие им описания.
[OOTB] Gardatech Garda Monitor application protocol	table	Таблица содержит идентификаторы протоколов и соответствующие им имена.
[OOTB] Gardatech Garda Monitor transport protocol	table	Таблица содержит идентификаторы протоколов и соответствующие им имена.
[OOTB] Gardatech Perimeter	table	Таблица содержит значения eventclassid и соответствующие ему значения полей Name.
[OOTB] H3C module names	dictionary	Словарь содержит значения кодов модулей маршрутизаторов H3C и соответствующие им описания модулей.
[OOTB] HTTP. Status codes	table	Таблица содержит коды состояния HTTP и соответствующие им имена.
[OOTB] InfoWatch Person Monitor. Operations names	table	Таблица содержит идентификаторы событий InfoWatch Person Monitor и соответствующие им имена.
[OOTB] Linux. Auditd record types	table	Словарь содержит идентификаторы событий ОС Linux и соответствующие им названия.
[OOTB] Microsoft DNS Server. EventIDs and Event Names	dictionary	Словарь содержит идентификаторы событий Microsoft DNS Server (из журнала Microsoft - Windows - DNS-Server – Audit) и соответствующие имена событий.
[OOTB] Microsoft Office 365. Event names	dictionary	Словарь содержит имена событий Microsoft Office 365.
[OOTB] Microsoft Office 365. User Type	dictionary	Словарь содержит сопоставления номеров типов пользователей с их текстовыми значениями Microsoft Office 365.
[OOTB] OrionSoft Termit event descriptions	table	Таблица содержит имена событий OrionSoft Termit и соответствующие им описания.
[OOTB] VK WorkSpace. Mail Event descriptions	table	Таблица содержит идентификаторы типов событий VK WorkSpace. Mail и соответствующие им описания.
[OOTB] Veeam Backup. EventIDs and Event Names	dictionary	Словарь содержит идентификаторы событий Veeam Backup и соответствующие имена событий.
[OOTB] Windows Hyper-V EventID-Name	dictionary	Словарь содержит идентификаторы событий Microsoft Hyper-V и соответствующие им имена событий.
[OOTB] Windows. FailureCodes (4625)	dictionary	Словарь содержит идентификаторы из полей "Failure Information\Status", "Failure Information\Sub Status" события 4625 Microsoft Windows и соответствующие им описания.
[OOTB] Windows. GroupPolicy EventIDs and Event Names mapping	table	Таблица содержит идентификаторы событий аудита групповых политик ОС Windows и соответствующие им имена событий.
[OOTB] Windows. Task category codes	dictionary	Словарь содержит идентификаторы параметра Task Category событий аудита ОС Windows и соответствующие им имена.
[OOTB] Windows_Sysmon. EventIDs and Event Names mapping	dictionary	Словарь содержит идентификаторы событий Sysmon и соответствующие имена событий.
[OOTB] Yandex Cloud	table	Таблица содержит идентификаторы сервисов Yandex Cloud и соответствующие им имена.
[OOTB] Zabbix. ResourceType	table	Словарь содержит идентификаторы ресурсов Zabbix и соответствующие им наименования.
[OOTB] NPO Fractel SSPT-4. Event names	table	Данная таблица содержит идентификаторы событий системы НПО Фрактел ССПТ-4А1 и соответствующие им имена событий.

Чтобы создать словарь:

1. В веб-интерфейсе решения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Словари** и нажмите кнопку **Создать**.

2. В поле **Название** укажите уникальное имя словаря. Максимальная длина имени: до 128 символов в кодировке Unicode.

3. В раскрывающемся списке **Тенант** выберите **тенант**, которому принадлежит словарь.

4. В поле **Описание** введите описание словаря. Максимальная длина описания: до 4000 символов в кодировке Unicode.

5. В раскрывающемся списке **Теги** выберите теги для словаря.

6. В раскрывающемся списке **Тип** выберите тип словаря:

   - **Словарь**

     Вы можете добавлять пары **Ключ** – **Значение**. Мы не рекомендуем добавлять в словари этого типа более 50 000 записей через веб-интерфейс.

     > При добавлении в словарь строк с одинаковыми ключами каждая новая строка будет записана поверх уже существующей строки с тем же самым ключом. В итоге в словарь будет добавлена только одна строка.

   - **Таблица**

     Вы можете добавлять данные в виде сложных таблиц и взаимодействовать с такими словарями через REST API. При добавлении записей через API ограничение на их количество отсутствует. REST API позволяет считывать и изменять содержимое словарей типа **Таблица**, даже если они используются активными сервисами. Это дает возможность использовать для обогащения событий динамически обновляемые таблицы, загружаемые из сторонних приложений.

7. В блоке параметров **Значение** настройте следующие параметры:

   - Если вы хотите загрузить готовый файл со словарем, выберите вариант **Импортировать CSV** и импортируйте файл.

     Формат CSV-файла зависит от типа словаря:

     Для типа **Словарь**:

     ```
     {КЛЮЧ},{ЗНАЧЕНИЕ}\n
     ```

     Для типа **Таблица**:

     ```
     {Заголовок столбца 1},{Заголовок столбца N},{Заголовок столбца N+1}\n
     {Ключ1},{ЗначениеN},{ЗначениеN+1}\n
     {Ключ2},{ЗначениеN},{ЗначениеN+1}\n
     ```

     Ключи должны быть уникальными как в импортируемом CSV-файле, так и в словаре. В таблицах ключ указывается в первом столбце. Длина ключа должна составлять от 1 до 128 символов Unicode, значения – от 0 до 256 символов Unicode.

     При импорте данные словаря полностью перезаписываются содержимым файла, а название ресурса заменяется именем импортированного файла.

Если в импортируемом файле обнаружены некорректные строки (например, содержащие неверные разделители), то при импорте в словарь такие строки пропускаются, а при импорте в таблицу вызывают ошибку и остановку процесса импорта.

- Если вы хотите добавить данные словаря вручную, выберите вариант **Ввести данные вручную** и выполните следующие действия в зависимости от выбранного типа словаря:

  - Для типа **Словарь** добавьте пары **Ключ** – **Значение**.

    Укажите уникальный ключ и соответствующее значение. При необходимости вы можете добавить несколько пар. Чтобы добавить новую строку таблицы, нажмите кнопку **Добавить строку**.

    Максимальная длина ключа: 128 символов в кодировке Unicode, а длина значения – 255 символов в кодировке Unicode. Первый символ ключа и значения не может быть $.

    Чтобы удалить строку, установите флажок напротив этой строки и нажмите кнопку **Удалить**.

  - Для типа **Таблица** введите данные таблицы.

    Введите данные таблицы. Вы можете добавлять и удалять строки и столбцы, а также изменять заголовки столбцов.

    Чтобы добавить новую строку или столбец, нажмите кнопку **Добавить строку** или **Добавить столбец**. Чтобы удалить строку, установите флажок напротив этой строки и нажмите кнопку **Удалить**. Чтобы удалить столбец, нажмите значок с тремя точками рядом с заголовком столбца и выберите **Удалить**.

8. Нажмите кнопку **Создать**.

После создания словаря вы можете экспортировать его, нажав **Экспортировать CSV** в окне редактирования. При экспорте значения ключей и значений, содержащие запятую (,) или кавычки ("), заключаются в двойные кавычки. Внутренние кавычки экранируются удвоением (""").

Настройка детектирующей логики и правил корреляции

Коррелятор – это компонент решения, который анализирует нормализованные события. В процессе корреляции может использоваться информация из активных листов и/или словарей.

Полученные в ходе анализа данные применяются для выполнения следующих задач:

- выявление алертов;
- уведомление о выявленных алертах;
- управление содержимым активных листов;
- отправка корреляционных событий в настроенные точки назначения.

Корреляция событий выполняется в реальном времени. Принцип работы коррелятора основан на сигнатурном анализе событий. Это значит, что каждое событие обрабатывается в соответствии с правилами корреляции, созданными пользователем.

При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции, коррелятор создает корреляционное событие. В зависимости от настроенной конфигурации корреляционное событие может быть отправлено в настроенную точку назначения, передано на повторный анализ в коррелятор или использовано для дальнейшей обработки.

Корреляционное событие можно отправлять на повторный анализ в коррелятор, позволяя таким образом настраивать правила корреляции на срабатывание от предыдущих результатов анализа. Результаты одного корреляционного правила могут использоваться другими корреляционными правилами.

Правила корреляции и используемые ими ресурсы можно распределять между корреляторами, чтобы разделять нагрузку между сервисами. Особенности распределения нагрузки зависят от используемой реализации коррелятора.

Алгоритм работы коррелятора

Алгоритм работы коррелятора состоит из следующих этапов:

1 Получение события

Коррелятор получает нормализованное событие от коллектора или другого сервиса.

2 Применение правил корреляции

Коррелятор анализирует полученное событие на соответствие условиям правил корреляции. Правила могут быть настроены для анализа отдельных событий или последовательностей событий. Если условия правила выполнены, коррелятор формирует результат корреляции и выполняет действия, заданные конфигурацией правила.

3 Обработка результата корреляции

В зависимости от конфигурации правила коррелятор может выполнять следующие действия:

- обогащать событие;
- выполнять операции с активными листами;
- выполнять операции с контекстными таблицами;
- формировать корреляционное событие;
- передавать результат на дальнейшую обработку.

Дополнительные действия могут выполняться с помощью настроенных правил обогащения, реагирования и маршрутизации.

4 Отправка корреляционного события

Если в результате анализа выявлена последовательность событий, удовлетворяющая условиям правила корреляции, коррелятор создает корреляционное событие.

В зависимости от конфигурации коррелятора корреляционное событие может быть отправлено в настроенную точку назначения или передано на повторный анализ в коррелятор. При повторном анализе корреляционное событие может использоваться другими правилами корреляции.

Создание коррелятора

Вы можете создать коррелятор в веб-консоли одним из следующих способов:

- В разделе **Мониторинг** → **Ресурсы и сервисы** нажмите **Создать коррелятор**.
- В разделе **Мониторинг** → **Ресурсы и сервисы** → **Корреляторы** нажмите **Создать**.

Создание коррелятора состоит из следующих этапов:

1 Настройка основных параметров коррелятора

1. В разделе **Общие** на вкладке **Основные параметры** заполните следующие поля:
   - В поле **Имя** введите уникальное имя коррелятора. Название должно содержать от 1 до 128 символов в кодировке Unicode.
   - При необходимости в поле **Обработчики** укажите количество обработчиков, которые коррелятор может запускать одновременно для параллельной обработки событий. Укажите целое положительное число от 0 до 999. Если указано 0, то используется число логических ядер CPU.
   - В поле **Время загрузки геоданных** укажите максимальное время ожидания загрузки геоданных (GeoIP-информации) при выполнении правил обогащения с типом источника данных **геоданные**. Значение по умолчанию: 120 секунд.
   - При необходимости в раскрывающемся списке **Теги** выберите теги для коррелятора.
   - При необходимости в поле **Описание** добавьте описание сервиса: до 256 символов в кодировке Unicode.
2. На вкладке **Дополнительные параметры** в поле **Число входящих запросов в очереди** укажите максимальное число запросов на вставку событий в базу данных, которые могут одновременно находиться в очереди на обработку коррелятором.

❷ Добавление глобальных переменных

Если для некоторых сценариев обеспечения безопасности недостаточно отслеживать значения в полях событий, активных листах или словарях, вы можете воспользоваться глобальными и локальными переменными. Эти переменные позволяют выполнять различные действия над поступающими в корреляторы значениями, реализуя сложную логику выявления угроз. Переменным можно присвоить какую-либо функцию, а затем обращаться к ним из правил корреляции, как к обычным полям событий, получая в ответ результат срабатывания функции.

Чтобы добавить глобальную переменную в коррелятор:

1. В разделе **Глобальные переменные** нажмите на кнопку **Добавить**.

2. Укажите следующие параметры:

   a. В окне **Переменная** введите название переменной.

   Требования к наименованию переменных

   - Должно быть уникально в рамках коррелятора.
   - Должно содержать от 1 до 128 символов в кодировке Unicode.
   - Не может начинаться с символа $.
   - Должно быть написано в camelCase или CamelCase.

   b. В окне **Значение** введите функцию переменной.

   При вводе функций поддерживается автодополнение в виде списка подсказок с возможными вариантами имен функций, их кратким описанием и примерами использования. Вы можете выбрать нужную функцию из списка и вставить ее вместе со списком аргументов в поле ввода.

   Для вызова списка всех подсказок в поле ввода используйте комбинацию клавиш **`Ctrl + Space`**. Для выбора нужной функции из списка используйте клавишу **`Enter`**. Для перехода к следующему аргументу в списке аргументов выбранной функции используйте клавишу **`Tab`**.

   Описание функций переменных.

Глобальная переменная добавлена. К ней можно обращаться из правил корреляции, добавляя перед названием переменной символ $. Переменных может быть несколько. Добавленные переменные можно изменить или удалить с помощью значка ✕.

❸ Добавление правила корреляции

Вы можете выбрать или создать правила корреляции. В них задаются последовательности событий, указывающих на происшествия, связанные с безопасностью: при обнаружении таких последовательностей коррелятор создает корреляционное событие и алерт.

Если вы добавили в коррелятор глобальные переменные, все добавленные правила корреляции могут к ним обращаться.

Чтобы добавить правило корреляции:

1. В разделе **Корреляция** нажмите на кнопку **Добавить**.

2. Укажите параметры для правила корреляции. Набор доступных параметров зависит от выбранного типа правила корреляции:

   - standard
   - simple
   - operational

   Правило корреляции создано и привязано к набору ресурсов для коррелятора. Оно отображается в таблице правил корреляции, а также в списке ресурсов в разделе **Мониторинг → Ресурсы и сервисы → Правила корреляции**.

С помощью поля **Поиск** можно искать правила корреляции. Добавленные правила корреляции можно убрать из набора ресурсов, выбрав нужные правила и нажав **Удалить**.

При выборе правила корреляции открывается окно с его параметрами: параметры можно изменить и **Сохранить**. При нажатии в этом окне на кнопку **Удалить**, правило корреляции отвязывается от набора ресурсов.

С помощью кнопок **Поднять** и **Опустить** можно изменять положение выбранных правил корреляции в таблице правил корреляции, что отражается на последовательности их выполнения при обработке событий. С помощью кнопки **Поднять operational-правила** можно переместить правила корреляции типа **operational** в начало списка правил корреляции.

4 Обогащение событий (необязательный этап)

Вы можете выбрать или создать правила обогащения с указанием, какими данными и из каких источников следует дополнить создаваемые коррелятором корреляционные события. Правил обогащения может быть несколько. Их можно добавить с помощью кнопки **Добавить обогащение** или удалить с помощью кнопки ×.

Чтобы добавить правило обогащения:

1. В разделе **Обогащение** нажмите на кнопку **Добавить обогащение**.

2. В раскрывающемся списке **Правило обогащения** выберите нужное правило или создайте новое, нажав **Создать**.

   Если вы выбрали правило обогащения из списка, то в разделе **Обогащение** отобразятся параметры выбранного правила.

3. В поле **Название** укажите уникальное название для правила обогащения.

4. В раскрывающемся списке **Тип источника данных** выберите, откуда будут поступать данные для обогащения, и заполните относящиеся к нему параметры:

   шаблон

   Этот тип обогащения используется, если в поле события нужно записать значение, полученное при обработке шаблонов Go. Мы рекомендуем сопоставлять значение и размер поля. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "шаблон"

Параметр	Описание
Шаблон	Шаблон Go. Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт, например `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.
Целевое поле	Поле события, в которое требуется поместить данные.

Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **шаблон**, целевым полем является поле с типом `Строка`, а исходным полем является поле расширенной схемы событий, содержащее массив строк, то в шаблоне может быть использован один из следующих примеров:

- `{{.SA.StringArrayOne}}`
- ```
  {{- range $index, $element := . SA.StringArrayOne -}}
  {{- if $index}}, {{end}}"{{$element}}"{{- end -}}
  ```

Для преобразования в шаблоне данных поля массива в формат TSV требуется использовать функцию `toString`, например:

```
template {{toString .SA.StringArray}}
```

таблица

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "таблица"

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.
Сопоставление	Поля событий для передачи данных: • **Поле словаря** – поля словаря, из которых будут передаваться данные. Доступные поля зависят от выбранного ресурса словаря. • **Поле KUMA** – поля событий, в которые будут передаваться данные. Для выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** вы можете задать название для помещаемых данных.

Первое поле в таблице (**Поле словаря**) считается ключом, с которым будут сопоставляться поля, выбранные из события в качестве ключевых (**Поле KUMA**). В качестве ключа в **Поле словаря** вам нужно выбрать индикатор компрометации, по которому будет осуществляться обогащение, например IP-адрес, URL-адрес или хеш. В правиле необходимо выбрать поле события, соответствующее выбранному индикатору в поле словаря.

Если вы хотите выбрать несколько ключевых полей, вы можете указать их через разделитель `|` (при указании через веб-интерфейс или импорте через CSV-файл), например `<IP-адрес>|<имя пользователя>`.

Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить**. Для удаления строки таблицы нажмите на крестик ✕.

константа
```

Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "константа"

Параметр	Описание
Константа	Значение, которое требуется добавить в поле события. Максимальная длина значения – до 255 символов в кодировке Unicode. Если оставить поле пустым, существующее значение поля события будет удалено.
Целевое поле	Поле события, в которое требуется поместить данные.

Если вы используете функции обогащения событий для полей расширенной схемы с типом `Строка`, `Число` или `Число с плавающей точкой` с помощью константы, в поле будет добавлена константа.

Если вы используете функции обогащения событий для полей расширенной схемы с типом `Массив строк`, `Массив чисел` или `Массив чисел с плавающей точкой` с помощью константы, константа будет добавлена к элементам массива.

словарь

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "словарь"

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.

Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **словарь**, а в параметре **Ключевые поля обогащения** указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку в соответствии с правилами сериализации одного значения в формате TSV.

Пример. В параметре **Ключевые поля обогащения** используется поле расширенной схемы `SA.StringArrayOne`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`. В качестве ключа в словарь будут переданы значения `['a','b','c']`.

Если в параметре **Ключевые поля обогащения** используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом `|`.

Пример. В параметре **Ключевые поля обогащения** используется поле расширенной схемы `SA.StringArrayOne` и строковое поле `Code`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`, а строковое поле `Code` содержит последовательность символов `myCode`. В качестве ключа в словарь будут переданы значения `['a','b','c']|myCode`.

событие

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры типа обогащения описаны в таблице ниже.

Параметры типа обогащения "событие"

Параметр	Описание
Целевое поле	Поле события, в которое следует поместить данные.
Исходное поле	Поле события, значение которого будет записано в целевое поле.
Преобразование	Блок параметров, в котором можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий. Тип преобразования можно выбрать в раскрывающемся списке. С помощью кнопок **Добавить преобразование** и **Удалить** можно добавить или удалить преобразование. Порядок преобразований имеет значение.

Возможность использовать преобразования зависит от типа используемого поля расширенной схемы событий:

- Для дополнительного поля с типом `Строка` доступны все типы преобразования.
- Для полей с типами `Число` и `Число с плавающей точкой` доступны типы преобразования **regexp**, **substring**, **replace**, **trim**, **append**, **prepend**, **replaceWithRegexp**, **decodeHexString**, **decodeBase64String** и **decodeBase64URLString**.
- Для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны типы преобразования **append** и **prepend**.

Посмотреть доступные преобразования

Преобразования – это изменения, которые применяются к значению перед записью в поле события.

Вы можете выбрать в раскрывающемся списке один из следующих типов преобразования:

- **entropy** – используется для преобразования значения исходного поля с помощью функции вычисления информационной энтропии и помещения результата преобразования в целевое поле типа `float`. Результатом преобразования будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например, когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.
- **lower** – используется для перевода всех символов значения в нижний регистр.
- **upper** – используется для перевода всех символов значения в верхний регистр.
- **regexp** – используется для преобразования значения с помощью указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.
- **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
  - **Символы на замену** – последовательность символов, которую требуется заменить.
  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

- **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` требуется выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.

- **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

- Конвертация закодированных строк в текст:

  - **decodeHexString** – используется для конвертации HEX-строки в текст.

  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  - **unicodeUnescape** – используется для конвертации Unicode-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.

  Мы не рекомендуем использовать несколько дополнительных нормализаторов для последовательного преобразования одного и того же поля. Результат одного преобразования, выполненного дополнительным нормализатором, не используется как входные данные для следующего. В итоговое событие записывается значение, полученное в дополнительном нормализаторе, который первым выполнил обогащение этого поля.

- Преобразование формата IP-адреса в IPv4:

  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.

  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.

- **hexToDecimal** – используется для преобразования числового значения, представленного в шестнадцатеричной системе счисления, в десятичный формат. Преобразование применяется к строковым или числовым полям, содержащим HEX-значения (включая префикс 0x, если он присутствует), и результат записывается в целевое поле события Kaspersky SIEM Cloud в виде целого числа.

  Результатом преобразования является число в десятичной системе, например исходное значение – 0x00FF, после преобразования – 255.

dns

Этот тип обогащения используется для отправки запросов на DNS-сервер частной сети для преобразования IP-адресов в доменные имена или наоборот. Преобразование IP-адресов в DNS-имена происходит только для частных адресов: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10, fd00::/8.

Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "dns"

Параметр	Описание
URL	URL DNS-сервера, которому вы хотите отправлять запросы. С помощью кнопки **Добавить URL** можно указать несколько URL. Если параметр **URL** не указан, то Kaspersky SIEM Cloud возьмет список DNS-серверов из файла `/etc/resolv.conf`, расположенного на локальном хосте. В этом случае вам нужно включить параметр **Требуется рекурсия**. В противном случае обогащение происходить не будет.
Запросов в секунду	Максимальное количество запросов к DNS-серверу в секунду. Значение по умолчанию: количество vCPU сервера, на котором установлено Ядро Kaspersky SIEM Cloud.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Укажите целое положительное число от 0 до 999. Если указано 0, то используется число логических ядер CPU. Значение по умолчанию: `1`.
Максимальное число событий в очереди обогащения	Максимальное число событий, сохраняемое в очереди для повторной отправки. Значение по умолчанию: `1 000 000`.
Время ожидания	Время ожидания ответа от DNS-сервера (в секундах). Значение по умолчанию: `5`.
Переопределение режима DNS	Используемый метод преобразования: • **Только прямое разрешение DNS** – доменное имя преобразуется в IP-адрес. • **Только обратное разрешение DNS** – IP-адрес преобразуется в доменное имя. • **Прямое и обратное DNS-разрешение** – доменное имя может преобразовываться в IP-адрес и наоборот.
Срок жизни кеша	Время жизни значений (в секундах), хранящихся в кеше. Значение по умолчанию: `60` (сек).
Кеш отключен	Параметр, позволяющий включить или выключить кеширование. По умолчанию кеширование включено.
Обновление кэша отключено	Если обновление кеша включено, то по истечении срока жизни кеша коллектор отправляет повторные запросы на DNS-сервер для обновления хранящихся в кеше данных. Этот параметр доступен только при включенном кеше. По умолчанию обновление кеша включено.
Требуется рекурсия	Параметр позволяет включить отправку коллектором рекурсивных запросов к авторитативным DNS-серверам для выполнения обогащения. Значение по умолчанию: **Выключено**.

cybertrace

Для систем с большой нагрузкой на коллектор или коррелятор рекомендуется использовать тип обогащения **cybertrace-http**. Этот тип обогащения возвращает структурированный ответ в формате JSON и корректно различает строки и массивы пользовательских атрибутов, исключая ошибки парсинга.
При обогащении с помощью типа **cybertrace** коллектор получает неструктурированный ответ. Если значение пользовательского атрибута в Kaspersky CyberTrace содержит квадратные скобки, например **[str1**, **str2]**, Kaspersky SIEM Cloud обрабатывает его как массив, а не как строку.

Этот тип обогащения используется для добавления в поля события сведений из потоков данных Kaspersky CyberTrace. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "cybertrace"

Параметр	Описание
URL	URL сервера Kaspersky CyberTrace, которому вы хотите отправлять запросы. Порт Kaspersky CyberTrace по умолчанию: 9999. Обязательный параметр.
Количество подключений	Максимальное количество подключений к серверу Kaspersky CyberTrace, которые может одновременно установить Kaspersky SIEM Cloud. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро Kaspersky SIEM Cloud.
Запросов в секунду	Максимальное количество запросов к серверу в секунду. Значение по умолчанию: `1000`.
Время ожидания	Время ожидания отклика от сервера Kaspersky CyberTrace в секундах. Значение по умолчанию: `30`.
Максимальное кол-во событий в очереди обогащения	Максимальное количество событий, сохраняемое в очереди для переотправки. Значение по умолчанию: `1 000 000`.
Сопоставление	Таблица сопоставления полей событий с типами индикаторов Kaspersky CyberTrace. В столбце **Поле KUMA** указаны названия полей событий, а в столбце **Индикатор CyberTrace** указаны типы индикаторов Kaspersky CyberTrace. Доступные типы индикаторов Kaspersky CyberTrace: • **ip** • **url** • **hash**

В таблице сопоставления требуется указать как минимум одну строку. Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить строку**. Для удаления строки таблицы нажмите на крестик ✕.

cybertrace-http

Этот тип потокового обогащения событий в Kaspersky CyberTrace, который позволяет отправлять большое количество событий одним запросом на API-интерфейс CyberTrace. Мы рекомендуем применять тип обогащения **cybertrace-http** в системах с большим потоком событий. Производительность **cybertrace-http** превосходит показатели типа обогащения **cybertrace**.

Ограничения:

- Тип обогащения **cybertrace-http** невозможно использовать для ретроспективного сканирования в KUMA.
- В случае использования типа обогащения **cybertrace-http** обнаружения киберугроз не сохраняются в истории Kaspersky CyberTrace в окне **Обнаружения**.

Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "cybertrace-http"

Параметр	Описание
Тенант	Тенант, в рамках которого вы планируете работать с Kaspersky CyberTrace. Обязательный параметр.
URL	URL сервера Kaspersky CyberTrace, которому вы хотите отправлять запросы и порт, который использует API CyberTrace. Порт по умолчанию 443. Обязательный параметр.
Секрет	Раскрывающийся список для выбора секрета, в котором хранятся учетные данные для подключения. Обязательный параметр.
Время ожидания	Время ожидания отклика от сервера Kaspersky CyberTrace в секундах. Значение по умолчанию: `30`.
Ключевые поля	Список полей событий, используемых для обогащения событий данными из Kaspersky CyberTrace. Обязательный параметр.
Максимальное кол-во событий в очереди обогащения	Максимальное количество событий, сохраняемое в очереди для переотправки. Значение по умолчанию: `1 000 000`. По достижении 1 млн получаемых событий от сервера Kaspersky CyberTrace события перестают обогащаться, пока число получаемых событий не станет меньше 500 тыс.
Основная версия CyberTrace	Версия Kaspersky CyberTrace. Доступные значения: • **<5** – запросы будут выполняться в тенанте General в Kaspersky CyberTrace и будут использовать новую версию API, соответствующую Kaspersky CyberTrace 5.0 и выше. • **≥ 5.0** – запросы будут использовать версию API, соответствующую Kaspersky CyberTrace 4.x. Значение по умолчанию: **<5**.
Отладка	Параметр, включающий логирование ресурса. По умолчанию переключатель выключен.
Теги	Теги для поиска ресурса.

часовой пояс

Этот тип обогащения используется в коллекторах и коррелляторах, чтобы присвоить событию определенный часовой пояс. Сведения о часовом поясе могут понадобиться при поиске событий, случившихся в нетипичное время, например ночью.

При выборе этого типа обогащения в раскрывающемся списке **Часовой пояс** нужно указать временную зону.

> Убедитесь, что выбираемый часовой пояс установлен на сервере сервиса, использующего обогащение. Например, это можно сделать с помощью команды `timedatectl list-timezones`, которая показывает все установленные на сервере часовые пояса. Подробнее об установке часовых поясов смотрите в документации используемой вами операционной системы.

При обогащении события в поле события DeviceTimeZone записывается смещение времени выбранного часового пояса относительно всемирного координированного времени (UTC) в формате `+-чч:мм`. Например, если выбрать временную зону **Asia/Yekaterinburg** в поле `DeviceTimeZone` будет записано значение `+05:00`. Если в обогащаемом событии есть значение поля `DeviceTimeZone`, оно будет перезаписано.

По умолчанию, если в обрабатываемом событии не указан часовой пояс и не настроены правила обогащения по часовому поясу, событию присваивается часовой пояс сервера, на котором установлен сервис (коллектор или коррелятор), обрабатывающий событие. При изменении времени сервера сервис требуется перезапустить.

Допустимые форматы времени при обогащении поля DeviceTimeZone

При обработке в коллекторе поступающих сырых событий следующие форматы времени могут быть автоматически приведены к формату `+-чч:мм` (см. таблицу ниже):

Формат времени в обрабатываемом событии	Пример
+-чч:мм	-07:00
+-ччмм	-0700
+-чч	-07

Если формат даты в поле `DeviceTimeZone` отличается от указанных в таблице, при обогащении события сведениями о часовом поясе в поле записывается часовой пояс серверного времени коллектора. Вы можете создать правила нормализации для нестандартных форматов времени.

геоданные

Этот тип обогащения используется для добавления в поля событий сведений о географическом расположении IP-адресов.

При выборе этого типа в блоке параметров **Сопоставление геоданных с полями события** укажите, из какого поля события будет считан IP-адрес, а также выберите атрибуты геоданных и определите поля событий, в которые геоданные будут записаны:

1. В раскрывающемся списке **Поле события с IP-адресом** выберите поле события, из которого считывается IP-адрес. По этому IP-адресу будет произведен поиск соответствий по загруженным в Kaspersky SIEM Cloud геоданным.

   > При выборе полей события `SourceAddress`, `DestinationAddress` и `DeviceAddress` становится доступна кнопка **Применить сопоставление по умолчанию**. С ее помощью можно добавить преднастроенные пары соответствий атрибутов геоданных и полей события.

2. Для каждого поля события, откуда требуется считать IP-адрес, выберите тип геоданных и поле события, в которое следует записать геоданные.

   - В поле **Атрибут геоданных** выберите, какие географические сведения, соответствующие считанному IP-адресу, необходимо записать в событие. Доступные атрибуты геоданных: **Страна**, **Регион**, **Город**, **Долгота**, **Широта**.
   - В поле **Поле события для записи** выберите поле события, в которое необходимо записать выбранный атрибут геоданных.

   С помощью кнопки **Добавить атрибут геоданных** вы можете добавить пары полей **Атрибут геоданных – Поле события для записи**. Так вы можете настроить запись разных типов геоданных одного IP-адреса в разные поля события.

3. Для добавления каждого последующего сопоставления используйте кнопку **Добавить сопоставление** и повторяйте предыдущие два пункта инструкции.

   Вы можете записать одинаковые атрибуты геоданных в разные поля событий. Если вы настроите запись нескольких атрибутов геоданных в одно поле события, событие будет обогащено последним по очереди сопоставлением.

проверка DLL Hijacking

DLL Hijacking – это техника атаки, которая заключается в том, что на целевую систему доставляется уязвимое легитимное программное обеспечение вместе с вредоносной динамической библиотекой (DLL). Для обнаружения таких атак Kaspersky SIEM Cloud использует модуль AI. Модуль AI анализирует параметры запуска и исполнения программ и определяет подозрительные случаи запуска легитимного программного обеспечения с вредоносными библиотеками.

Для получения заключения Kaspersky SIEM Cloud отправляет запрос с информацией из полей события в <KSN>. В ответ на запрос KSN присылает результат анализа.

Вы можете настроить обнаружение атак DLL Hijacking в коллекторе или корреляторе.

Для использования обогащения типа **Проверка DLL Hijacking** ваша лицензия должна включать в себя модуль AI. Главному администратору также требуется принять дополнительное Положение о KSN в блоке **Kaspersky Security Network** (**Параметры** → **KUMA** → **Открыть параметры KUMA** → **Интеграции** → **AI-сервисы** → **Обнаружение атак DLL Hijacking**).

Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "DLL Hijacking"

Параметр	Описание
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Укажите целое положительное число от 0 до 999. Если указано 0, то используется число логических ядер CPU.
Максимальный размер кеша	Максимальный размер кеша для ответов, получаемых из KSN, в мегабайтах. Значение по умолчанию: `128 МБ`. Каждый ответ из KSN имеет свое время жизни, в течение которого он хранится в кеше. Если Kaspersky SIEM Cloud отправляет повторный запрос по файлу DLL, для которого KSN уже выдал ответ, и время жизни этого ответа еще не истекло, то запрос не отправляется в KSN, а ответ берется из кеша.
Максимальное количество событий в очереди обогащения	При превышении указанного значения, новые события обрабатываться не будут. Значение по умолчанию: `1 000 000`. Значение `0` означает, что при возникновении очереди события перестают обогащаться.

Выполнять повторный запрос	В ответе KSN может выдать заключение **В обработке**. Этот заключение означает, что KSN принял запрос и в данный момент обрабатывает его, но заключения пока нет. Обработка может занять длительное время, поэтому требуется повторная отправка запроса.
	Если этот параметр включен, настройте дополнительные параметры:
	• **Создавать дубликаты событий** – если этот параметр включен, Kaspersky SIEM Cloud создает дубликат события и использует его для повторных запросов к KSN. Основное событие при этом отправляется дальше по потоку. Дубликат события будет записан в базу данных, когда выполнится одно из следующих условий:
	  • Из KSN получено заключение, отличное от **В обработке**.
	  • Переполнен дисковый буфер, размер которого указан в параметре **Размер буфера**.
	  • Превышено значение, указанное в параметре **Количество запросов**.
	  Если этот параметр выключен, Kaspersky SIEM Cloud продолжит отправлять запросы с использованием основного события. Событие будет записано в базу данных, когда выполнится одно из следующих условий:
	  • Из KSN получено заключение, отличное от **В обработке**.
	  • Переполнен дисковый буфер, размер которого указан в параметре **Размер буфера**.
	  • Превышено значение, указанное в параметре **Количество запросов**.
	• **Количество запросов** – максимальное количество запросов в KSN. Если за указанное количество запросов так и не будет получено заключение, отличное от **В обработке**, событие будет записано в базу данных с заключением **В обработке**. Значение по умолчанию: `10`.
	• **Интервал запросов** – интервал между запросами, в минутах. Значение по умолчанию: `1 минута`. Минимальное значение: `1 минута`.
	• **Размер буфера** – размер дискового буфера, который используется для хранения событий, ожидающих повторного запроса, в мегабайтах. Значение по умолчанию: `10240 МБ`. Минимальное значение: `10 МБ`.

Прокси-сервер	Параметры прокси-сервера, если он требуется для подключения к серверу KSN. Можно выбрать один из доступных или создать новый прокси-сервер. По умолчанию прокси-сервер не используется.
Сопоставление	Таблица параметров, которые нужно отправить в запросе в KSN для получения заключения, и соответствующих полей событий Kaspersky SIEM Cloud: • **Хеш файла DLL (md5)** – рекомендованное поле для сопоставления: `OldFileHash`. • **Путь до файла DLL** – полный путь, включающий имя файла. Рекомендованное поле для сопоставления: `OldFilePath`. Так как путь может содержать персональные данные, Kaspersky SIEM Cloud передает этот параметр в KSN в обезличенном виде. Например: Путь до обезличивания: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll` Тот же путь в обезличенном виде: `device\harddiskvolume1\users\username` • **Хеш процесса (md5)** – рекомендованное поле для сопоставления: `FileHash`. • **Путь до процесса** – полный путь, включающий имя файла. Так как путь может содержать персональные данные, Kaspersky SIEM Cloud передает этот параметр в KSN в обезличенном виде. Например: Путь до обезличивания: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll` Тот же путь в обезличенном виде: `device\harddiskvolume1\users\username` • **Имя файла DLL** – рекомендованное поле для сопоставления: `OldFileName`. • **Имя процесса** – рекомендованное поле для сопоставления: `FileName`. • **Подпись процесса** – поле, в котором указывается поле Kaspersky SIEM Cloud, которое передает `Organization` из `Subject` подписи. Если этих значений нет, подпись стоит оставить пустой. Чтобы добавить этот параметр, нажмите на кнопку **Добавить**, затем в столбце **Поле DLL Hijacking** в выпадающем списке выберите **подпись процесса**.необязательный параметр. Рекомендованное поле для сопоставления: FileID. • **Размер файла DLL** – необязательный параметр; рекомендованное поле для сопоставления: OldFileSize. Чтобы добавить этот параметр, нажмите на кнопку **Добавить**, затем в столбце **Поле DLL Hijacking** в выпадающем списке выберите **размер файла DLL**. Для каждого параметра укажите в таблице соответствующее ему поле события Kaspersky SIEM Cloud.

5. В блоке **Параметры фильтров** можно задать условия определения событий, которые будут обрабатываться с применением правила обогащения. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр.

   Создание фильтра в ресурсах

   Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

   Чтобы создать фильтр:

   1. В раскрывающемся списке **Фильтр** выберите **Создать**.

   2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят.

   3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.

   4. Выберите режим создания фильтра: **Конструктор** или **Код**.

      При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра.

5. Если вы выбрали вариант **Конструктор**, выполните следующие действия:

a. В раскрывающемся списке выберите логический оператор:

- **И** – отбирает события, которые соответствуют всем указанным условиям.
- **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий.
- **НЕ** – отбирает события, которые не соответствуют всем указанным условиям.

b. Нажмите на кнопку **Добавить условие**.

c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра.

Операнды фильтров

- **Поля событий** – поле события, которое требуется использовать как операнд фильтра.
- **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**.

  Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра.

- **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры:
  - **словарь** (обязательно) – словарь, который требуется использовать.
  - **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.
- **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события.
  - **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать.
  - **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы.
  - **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда.
  - **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда.

- **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
  - **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**.
  - **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.
- **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
  - **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
  - **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
  - **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
- **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
  - **значение** (обязательно) – константа, которую требуется присвоить операнду.
- **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
  - **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.

Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.

- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.

- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.

- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.

- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.

- **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в коррелляторах.

- **inContextTable** – присутствует ли в указанной контекстной таблице запись.

- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.

Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.

e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.

Вы можете добавить несколько групп условий.

6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.

   В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕.

8. Нажмите **Сохранить**.

В набор ресурсов для коррелятора добавлено новое правило обогащения.

5 Добавление правила реагирования (необязательный этап)

Вы можете выбрать или создать правила реагирования с указанием, какие действия требуется выполнить при срабатывании правил корреляции. Правил реагирования может быть несколько. Их можно добавить с помощью кнопки **Добавить правило реагирования** или удалить с помощью кнопки ✕.

Чтобы добавить правило реагирования:

1. В разделе **Реагирование** нажмите на кнопку **Добавить правило реагирования**.

2. В раскрывающемся списке **Правило реагирования** выберите нужное правило или создайте новое, нажав **Создать**.

   Если вы выбрали правило реагирования из списка, то в разделе **Реагирование** отобразятся параметры выбранного правила.

3. В раскрывающемся списке **Тип** выберите **Запуск скрипта**.

   Вы можете создать скрипт с командами, которые требуется выполнить на сервере Kaspersky SIEM Cloud при обнаружении выбранных событий.

   Файл скрипта хранится на сервере, где установлен сервис коррелятора, использующий ресурс реагирования: `/opt/kaspersky/kuma/correlator/<correlator_ID>/scripts`. Пользователю `kuma` этого сервера требуются права на запуск скрипта.

   Параметры реагирования

   - **Время ожидания** – количество секунд, которое выждет система, прежде чем запустить скрипт.

   - **Название скрипта** (обязательно) – имя файла скрипта.

     Если ресурс реагирования прикреплен к сервису коррелятора, однако в папке /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts файл скрипта отсутствует, коррелятор не будет работать.

   - **Аргументы скрипта** – параметры или значения полей корреляционных событий, которые необходимо передать скрипту.

     > Если в скрипте производятся какие-либо действия с файлами, к ним следует указывать абсолютный путь.

     Параметры можно обрамлять кавычками (").

     Имена полей корреляционных событий передаются в формате `{{.EventField}}`, где `EventField` – это имя поля события, значение которого должно быть передано в скрипт.

     Пример: `-n "\"usr\": {{.SourceUserName}}"`

4. В поле **Обработчики** укажите количество обработчиков, которые коррелятор может запускать одновременно для параллельной обработки событий. Укажите целое положительное число от 0 до 999. Если указано 0, то используется число логических ядер CPU.

   Поле не обязательно для заполнения.

5. В блоке параметров **Фильтр** можно задать условия определения событий, которые будут обрабатываться с применением правила реагирования. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр.

   Создание фильтра в ресурсах

   Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

   Чтобы создать фильтр:

   1. В раскрывающемся списке **Фильтр** выберите **Создать**.

   2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят.

   3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.

   4. Выберите режим создания фильтра: **Конструктор** или **Код**.

      При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра.

   5. Если вы выбрали вариант **Конструктор**, выполните следующие действия:

      a. В раскрывающемся списке выберите логический оператор:

         - **И** – отбирает события, которые соответствуют всем указанным условиям.
         - **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий.
         - **НЕ** – отбирает события, которые не соответствуют всем указанным условиям.

      b. Нажмите на кнопку **Добавить условие**.

      c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

      d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра.

Операнды фильтров

- **Поля событий** – поле события, которое требуется использовать как операнд фильтра.

- **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**.

  Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра.

- **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры:

  - **словарь** (обязательно) – словарь, который требуется использовать.

  - **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.

- **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события.

  - **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать.

  - **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы.

  - **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда.

  - **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда.

- **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:

  - **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**.

  - **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.

- **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:

  - **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.

  - **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.

  - **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.

- **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
  - **значение** (обязательно) – константа, которую требуется присвоить операнду.
- **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
  - **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.

Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.

- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в коррелляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.

Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.

e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.

Вы можете добавить несколько групп условий.

6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.

В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕.

8. Нажмите **Сохранить**.

В набор ресурсов для коррелятора добавлено новое правило реагирования.

6 Добавление точки назначения (необязательный этап)

Вы можете выбрать или создать точки назначения, в параметрах которых будут определено, куда следует перенаправлять созданные коррелятором события. Обычно события от коррелятора перенаправляются в хранилище для хранения и для возможности просматривать их позднее. При необходимости события можно отправлять в другие места. Точек назначения может быть несколько.

Чтобы добавить точку назначения:

1. В разделе **Маршрутизация** нажмите на кнопку **Добавить**.

2. В открывшемся окне в поле **Точка назначения** выберите тип точки назначения, которую вы хотите добавить, или создайте новую, нажав **Создать** и настроив следующие параметры:

   a. На вкладке **Основные параметры** в поле **Название** введите уникальное имя точки назначения. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   b. С помощью переключателя **Состояние** вы можете при необходимости включить или выключить сервис.

   c. В раскрывающемся списке **Тип** выберите тип точки назначения. Доступны следующие значения:

      - internal
      - nats-jetstream
      - tcp
      - udp
      - http
      - diode
      - kafka
      - file
      - storage
      - correlator
      - eventRouter

   d. На вкладке **Дополнительные параметры** укажите значения для параметров настройки. Набор параметров для настройки зависит от типа точки назначения, выбранного на вкладке **Основные параметры**. Более подробная информация о параметрах и значениях доступна по ссылке для каждого типа точки назначения в пункте c. этой инструкции.

В набор ресурсов для коррелятора добавлена новая точка назначения.

7 Установка коррелятора в облачной инфраструктуре

На этом этапе в Kaspersky SIEM Cloud создается набор ресурсов для сервиса и на основе этого набора автоматически создаются сервисы:

- Набор ресурсов для коррелятора отображается в разделе **Мониторинг → Ресурсы и сервисы → Корреляторы**. Его можно использовать для создания новых сервисов коррелятора. При изменении этого набора ресурсов все сервисы, которые работают на его основе, будут использовать новые параметры, если сервисы перезапустить: для этого можно использовать кнопки **Сохранить и перезапустить сервисы** и **Сохранить и обновить параметры сервисов**.

  Набор ресурсов можно изменять, копировать, переносить из папки в папку, удалять, импортировать и экспортировать, как другие ресурсы.

- Сервисы отображаются в разделе **Мониторинг → Ресурсы и сервисы → Активные сервисы**.

После завершения создания и настройки коррелятора требуется установить коррелятор Kaspersky SIEM Cloud в облачной инфраструктуре.

Правила корреляции

Правила корреляции используются для распознавания определенных последовательностей обрабатываемых событий и выполнения определенных действий после распознавания: например, создание корреляционных событий или алертов, взаимодействие с активным листом.

Правила корреляции можно использовать в следующих сервисах и функциях Kaspersky SIEM Cloud:

- Коррелятор.
- Правило уведомления.
- Связи правил сегментации.
- Ретроспективное сканирование.

Доступные параметры правила корреляции зависят от выбранного типа. Типы правил корреляции:

- standard – используется для поиска корреляций между несколькими событиями. Правила этого типа могут создавать корреляционные события.

  Этот тип правил используется для определения сложных закономерностей в последовательности событий. Для более простых комбинаций следует использовать другие типы правил корреляции, которые требуют меньше ресурсов.

- simple – используется для создания корреляционных событий при обнаружении определенного события.

- operational – используется для операций с активными листами и контекстными таблицами. Этот тип правил не может создавать корреляционные события.

Для этих ресурсов в полях ввода, кроме поля **Описание**, можно включить отображение непечатаемых символов.

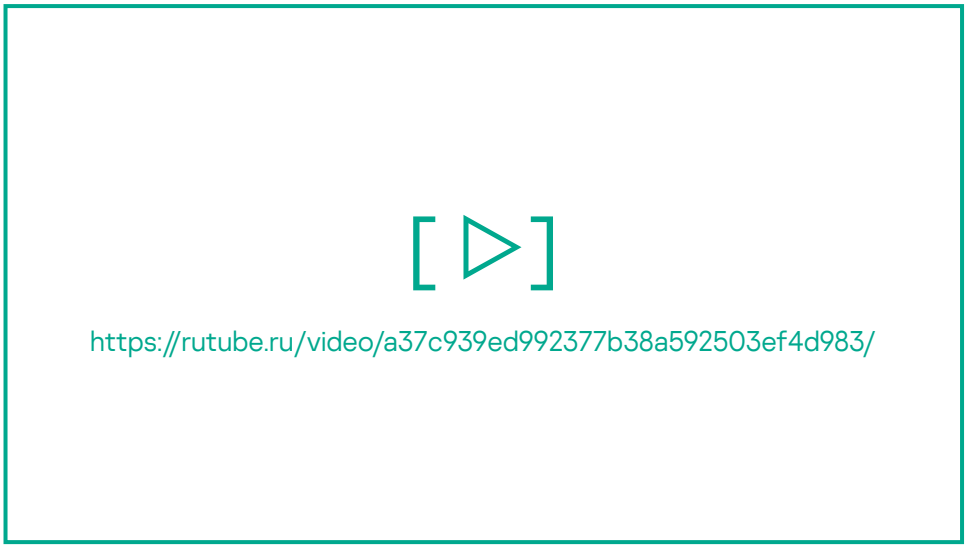
Если правило корреляции используется в коррелляторе и по нему был создан алерт, то при изменении правила корреляции существующий алерт не будет изменен, даже если перезапустить сервис коррелятора. Например, если у правила корреляции было изменено название, название алерта останется прежним. Если существующий алерт закрыть, то новый алерт будет создан уже с учетом изменений правила корреляции.

Если в правиле корреляции используется другой ресурс, например, сохраненный ранее фильтр, и этот ресурс изменяется, то при экспорте правила корреляции в файл могут попасть данные из более ранней версии измененного ресурса. При этом дальнейший импорт правила корреляции из этого файла завершается корректно, Kaspersky SIEM Cloud импортирует последнюю версию ресурса.

Работа с правилами корреляции

Вы можете создавать, копировать, изменять и удалять правила корреляции.

Для наглядного ознакомления с процессом создания правила корреляции вы можете просмотреть видео ниже, а затем воспользоваться пошаговой инструкцией.



https://rutube.ru/video/a37c939ed992377b38a592503ef4d983/

Создание правила корреляции

Чтобы создать правило корреляции:

1. В веб-интерфейсе откройте раздел **Мониторинг** → **Ресурсы и сервисы** → **Правила корреляции** и нажмите на кнопку **Создать**.

   Справа откроется панель создания правила корреляции.

2. На вкладке **Общие** выполните следующие действия:

   a. Введите имя ресурса в поле **Название**. Имя ресурса должно быть уникальным в рамках выбранного тенанта.

   b. В раскрывающемся списке **Тенант** выберите тенант, к которому будет относиться правило корреляции.

c. В раскрывающемся списке **Тип** выберите тип правила корреляции: **standard**, **simple** или **operational**.

d. При необходимости в раскрывающемся списке **Теги** добавьте теги.

e. Укажите частоту срабатывания правила корреляции.

f. При необходимости добавьте описание правила корреляции.

g. В раскрывающемся списке **Техники MITRE** выберите техники выявления угроз, которые будут применяться в правиле корреляции.

3. На вкладке **Селекторы** задайте условия срабатывания правила корреляции. Для этого выполните следующие действия:

   - На вкладке **Параметры** выполните одно из следующих действий:

     - В раскрывающемся списке **Фильтр** выберите или создайте фильтр для определения события, при котором будет срабатывать правило корреляции.

       Для сохранения выбранного фильтра установите флажок **Сохранить фильтр**.

     - Укажите условие для срабатывания правила корреляции с помощью конструктора (смотреть примеры).

     - Введите код условия для срабатывания правила корреляции.

   - При необходимости на вкладке **Локальные переменные** укажите локальные переменные для условия срабатывания правила.

4. На вкладке **Действия** добавьте операции по обновлению ресурсов.

5. Нажмите **Создать**.

Правило корреляции будет создано и доступно для использования в сервисах и других ресурсах.

Копирование правила корреляции

Чтобы скопировать правило корреляции:

1. В веб-интерфейсе откройте раздел **Мониторинг → Ресурсы и сервисы → Правила корреляции** и установите флажок рядом с правилом корреляции, которое вы хотите скопировать.

2. Нажмите **Дублировать**.

   В нижней части таблицы отобразится количество выбранных правил.

   Справа откроется панель с параметрами правила корреляции, которое вы выбрали для копирования.

   В поле **Название** отображается `<название выбранного правила корреляции> - копия`.

3. Измените нужные параметры (см. инструкцию по созданию правила корреляции).

4. Нажмите **Сохранить**.

Копия правила корреляции будет создана.

Изменение параметров правила корреляции

Чтобы изменить правило корреляции:

1. В веб-интерфейсе откройте раздел **Мониторинг → Ресурсы и сервисы → Правила корреляции** и нажмите на правило, которое вы хотите изменить

   Справа откроется панель с параметрами выбранного правила корреляции.

2. Измените нужные параметры (см. инструкцию по созданию правила корреляции).

3. Выполните одно из следующих действий:

   - Нажмите **Сохранить**, чтобы сохранить изменения.

   - Нажмите **Сохранить с комментарием** и в открывшемся окне укажите комментарий к внесенным изменениям. Изменения будут сохранены, и комментарий будет добавлен к созданной версии правила корреляции.

   Если при сохранении изменений обнаруживается, что текущая версия правила корреляции была изменена другим пользователем, вам будет предложен выбор из следующих действий:

   - Сохранить ваши изменения как новую версию поверх изменений другого пользователя.

   - Сохранить ваши изменения как новое правило корреляции.

     В этом случае будет создан дубликат изначального правила корреляции с измененными параметрами. В название нового правила будет добавлено `- копия`, и в комментарии к версии правила корреляции будут указаны название и версия ресурса, с которого был создан дубликат.

   - Отменить ваши изменения.

     Отмененные изменения невозможно восстановить.

   Правило корреляции будет обновлено. Если этот ресурс используется в сервисе, перезапустите сервис, чтобы он использовал новую версию правила корреляции.

Удаление правила корреляции

Чтобы удалить правило корреляции:

1. В веб-интерфейсе откройте раздел **Мониторинг → Ресурсы и сервисы → Правила корреляции** и установите флажок рядом с правилом корреляции, которое вы хотите удалить.

   В нижней части таблицы отобразится количество выбранных ресурсов.

2. Нажмите **Удалить**.

3. В открывшемся окне подтвердите удаление.

   Правило корреляции и все его сохраненные версии будут удалены.

Правило корреляции, тип standard

Правила корреляции с типом **standard** используются для определения сложных закономерностей в обрабатываемых событиях.

Поиск закономерностей происходит с помощью контейнеров

Контейнеры правила корреляции – это временные хранилища данных, которые используются ресурсами правила корреляции при определении необходимости создания корреляционных событий. Эти контейнеры выполняет следующие функции:

- Группируют события, которые были отобраны фильтрами в группе настроек **Селекторы** ресурса правила корреляции. События группируются по полям, которые указываются пользователем в поле **Группирующие поля**.
- Определяют момент, когда должно сработать правило корреляции, меняя соответствующим образом события, сгруппированные в контейнере.
- Выполняют действия, указанные в группе настроек **Действия**.
- Создают корреляционные события.

Доступные состояния контейнера:

- `Пусто` – в контейнере нет событий. Это может произойти только в момент своего создания при срабатывании правила корреляции.
- `Частичное совпадение` – в контейнере есть некоторые из ожидаемых событий (события восстановления не учитываются).
- `Полное совпадение` – в корзине есть все ожидаемые события (события восстановления не учитываются). При достижении этого состояния:
  - Срабатывает правило корреляции
  - События удаляются из контейнера
  - Счетчик срабатываний контейнера обновляется
  - Контейнера переводится в состояние `Пусто`
- `Ложное совпадение` – такое состояние контейнера возможно в следующих случаях:
  - когда было достигнуто состояние `Полное совпадение`, но объединяющий фильтр возвратил значение false.
  - когда при установленном флажке **Обнуление** были получены события восстановления.

  Когда это условие достигается, правило корреляции не срабатывает. События удаляются из контейнера, счетчик срабатываний обновляется, контейнер переводится в состояния `Пусто`.

Для правил корреляции установлено ограничение частоты срабатывания – одно срабатывание в секунду. Изменить частоту срабатывания правила невозможно.

По сравнению с моделью данных нормализованного события некоторые поля корреляционного события, образованного по правилу корреляции **standard**, могут отличаться (см. таблицу ниже).

Название поля корреляционного события	Описание
StartTime	Самая ранняя дата и время создания базового события (timestamp) среди всех базовых событий, от которых было образовано корреляционное событие.
EndTime	Более поздняя дата и время из следующих: • Дата и время создания корреляционного события. • Самая поздняя дата и время создания базового события (timestamp) среди всех базовых событий, от которых было образовано корреляционное событие.

Вы можете добавить в корреляционное событие поля из базовых событий, указав эти поля в параметрах **Группирующие поля** и **Уникальные поля** (см.таблицу ниже).

Доступные параметры правила корреляции с типом **standard** описаны в таблицах ниже.

Вкладка Общие

Эта вкладка используется для указания основных параметров правила корреляции.

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип правила корреляции – **standard**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Группирующие поля	Поля событий, которые должны быть сгруппированы в контейнере. Хеш-код значений выбранных полей событий используется в качестве ключа контейнера. Если срабатывает один из селекторов, указанных на вкладке **Селекторы**, отобранные поля событий копируются в корреляционное событие. Если в разных селекторах корреляционного правила используются поля событий, которые имеют разные значения в событиях, вам не нужно указывать эти поля событий в раскрывающемся списке **Группирующие поля**. Вы можете указывать локальные переменные. Для обращения к локальной переменной вам нужно указать перед ее именем символ `$`. Для ознакомления с примерами использования локальных переменных используйте правило **R403_Обращение на вредоносные ресурсы с хоста с отключенной защитой или устаревшей антивирусной базой**, поставляемое с Kaspersky SIEM Cloud. Обязательный параметр.
Время жизни контейнера, сек.	Время жизни контейнера в секундах. Отсчет времени начинается при создании контейнера, когда контейнер получает первое событие. По истечении времени жизни контейнера срабатывает триггер, указанный на вкладке **Действия → По истечении времени жизни контейнера**, и контейнер удаляется. Триггеры, указанные на вкладках **Действия → На каждом срабатывании правила** и **На последующих срабатываниях правила**, могут срабатывать более одного раза в течение времени жизни контейнера. Обязательный параметр.
Уникальные поля	Уникальные поля событий, которые требуется отправлять в контейнер. Если вы указываете уникальные поля событий, только они будут отправляться в контейнер. Хеш-код значений отобранных полей событий используется в качестве ключа контейнера. Вы можете указывать локальные переменные. Для обращения к локальной переменной вам нужно указать перед ее именем символ `$`. Для ознакомления с примерами использования локальных переменных используйте правило **R403_Обращение на вредоносные ресурсы с хоста с отключенной защитой или устаревшей антивирусной базой**, поставляемое с Kaspersky SIEM Cloud.

Параметр	Описание
Политика хранения базовых событий	Раскрывающийся список, позволяющий определить, какие базовые события требуется поместить в корреляционное событие: • **first** – поместить в корреляционное событие первое базовое событие из коллекции событий, инициировавшей создание корреляционного события. Это значение выбрано по умолчанию. • **last** – поместить в корреляционное событие последнее базовое событие из коллекции событий, инициировавшей создание корреляционного события. • **all** – поместить в корреляционное событие все базовые события из коллекции событий, инициировавшей создание корреляционного события.
Уровень важности	Базовый коэффициент, используемый для определения уровня важности правила корреляции: • **Критический**. • **Высокий**. • **Средний**. • **Низкий** – это значение выбрано по умолчанию.
Сортировать по	Поле события, по которому селекторы правила корреляции будут отслеживать изменение ситуации. Это может пригодиться, например если вы захотите настроить правило корреляции на срабатывание при последовательном возникновении нескольких типов событий.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.
Техники MITRE	Загруженные техники MITRE ATT&CK для анализа состояния покрытия безопасности с помощью матрицы MITRE ATT&CK.
Использовать сопоставление уникальных полей	Переключатель, позволяющий сохранять значения уникальных полей в массив и передавать его в одно из полей корреляционного события. Если переключатель включен, в нижней части вкладки **Общие** отображается дополнительный блок параметров **Сопоставление уникальных полей** для настройки сопоставления исходных уникальных полей с полями корреляционного события. При обработке события через правило корреляции сначала выполняется сопоставление полей, затем к уже сформированному на основе сопоставления корреляционному событию будут применены операции, указанные на вкладке **Действия**. По умолчанию переключатель выключен. Необязательный параметр.

Блок параметров Сопоставление уникальных полей

Если необходимо передавать в корреляционное событие значения полей, указанных в параметре **Уникальные поля**, то этот блок можно использовать для настройки сопоставления уникальных полей с полями корреляционного события. Блок отображается на вкладке **Общие**, если включен переключатель **Использовать сопоставление уникальных полей**. Поскольку значения уникальных полей представляют собой массив, поле в корреляционном событии должно иметь соответствующий тип – SA, NA, FA.

Вы можете добавить сопоставление, нажав на кнопку **Добавить** и выбрав в раскрывающемся списке в столбце **Поле исходного события** нужное поле. Для выбора доступны поля, указанные в параметре **Уникальные поля**. В раскрывающемся списке в столбце **Поле события назначения** вам нужно выбрать поле корреляционного события, в которое должен записываться массив значений исходного поля. Для выбора доступны поля, тип которых соответствует массиву (SA, NA или FA в зависимости от типа исходного поля).

Вы можете удалить одно или несколько сопоставлений, установив флажки рядом с нужными сопоставлениями и нажав на кнопку **Удалить**.

Вкладка Селекторы

Эта вкладка используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Для добавления селектора нажмите на кнопку **+ Добавить селектор**. Вы можете добавить несколько селекторов, изменить порядок селекторов и удалить селекторы. Для изменения порядка селекторов используйте значки изменения порядка ⣿. Для удаления селектора нажмите рядом с ним на значок удаления ✕.

Для каждого селектора доступны вкладки **Параметры** и **Локальные переменные**.

Параметры, доступные на вкладке **Параметры**, описаны в таблице ниже.

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Порог срабатывания селектора (количество событий)	Количество событий, которые требуется получить для срабатывания селектора. Значение по умолчанию: `1`. Обязательный параметр.

Обнуление	Переключатель, позволяющий правилу корреляции не срабатывать при получении селектором количества событий, указанного в поле **Порог срабатывания селектора (количество событий)**. По умолчанию этот переключатель выключен.
	Пример работы селектора с включенным переключателем Обнуление
	Переключатель **Обнуление** используется в селекторах правил корреляции для сброса контейнера и предотвращения создания корреляционного события. Чаще всего обнуление применяется вместе с действием **По истечении времени жизни контейнера**.
	Правило корреляции типа **standard** настроено следующим образом:
	• В поле **Время жизни контейнера** указано значение `300 секунд`.
	• На вкладке **Действия** настроен триггер **По истечении времени жизни контейнера** с установленным флажком **В дальнейшую обработку**.
	• В правило корреляции добавлено два селектора:
	  ◦ **Virus detected** (в примере событие `{"Message": "virus detected"}`) с выключенным переключателем **Обнуление**.
	  ◦ **Virus deleted** (в примере событие `{"Message": "virus deleted"}`) с включенным переключателем **Обнуление**.
	Когда поступает событие `{"Message": "virus detected"}`, запускается контейнер и происходит следующее:
	• В течение 300 секунд не поступает событие `{"Message": "virus deleted"}`. В этом случае контейнер закрывается и триггер создает корреляционное событие.
	• В течение 300 секунд поступает событие `{"Message": "virus deleted"}`, которое соответствует селектору с включенным переключателем **Обнуление**. В этом случае контейнер очищается и корреляционное событие не создается.

Параметр	Описание
Фильтр	Фильтр, указывающий критерии определения событий, при получении которых будет срабатывать селектор. Вы можете выбрать существующий фильтр или создать новый фильтр. Для создания нового фильтра выберите значение **Создать**. Если вы хотите изменить параметры существующего фильтра, нажмите рядом с ним на значок карандаша. Если вы будете использовать фильтр в других правилах корреляции, вам нужно сохранять его как отдельный ресурс. **Как создать фильтр?** Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. Выберите режим создания фильтра: **Конструктор** или **Код**. При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра. 5. Если вы выбрали вариант **Конструктор**, выполните следующие действия: a. В раскрывающемся списке выберите логический оператор: • **И** – отбирает события, которые соответствуют всем указанным условиям. • **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий. • **НЕ** – отбирает события, которые не соответствуют всем указанным условиям. b. Нажмите на кнопку **Добавить условие**. c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра. **Операнды фильтров** • **Поля событий** – поле события, которое требуется использовать как операнд фильтра. • **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**. Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра. • **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – словарь, который требуется использовать. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря. • **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события. • **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать. • **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы. • **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда. • **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда. • **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.

Параметр	Описание

	• **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
	  • **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
	  • **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
	  • **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
	• **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константа, которую требуется присвоить операнду.
	• **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
	Операторы фильтров
	• **=** – левый операнд равен правому операнду.
	• **<** – левый операнд меньше правого операнда.
	• **<=** – левый операнд меньше или равен правому операнду.
	• **>** – левый операнд больше правого операнда.
	• **>=** – левый операнд больше или равен правому операнду.
	• **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
	• **contains** – левый операнд содержит значения правого операнда.
	• **startsWith** – левый операнд начинается с одного из значений правого операнда.
	• **endsWith** – левый операнд заканчивается одним из значений правого операнда.
	• **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
	• **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).
	Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.
	Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
	• **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
	Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
	• **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
	• **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
	• **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
	• **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
	• **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись.
	• **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.
	Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.
	Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.
	e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.
	Вы можете добавить несколько групп условий.
	6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.
	В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

Параметр	Описание

	7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕.
	
	8. Нажмите **Сохранить**.
	
	Фильтрация по данным из поля события Extra
	
	Условия для фильтров по данным из поля события `Extra`:
	
	• Условие – **Если**.
	• Левый операнд – **поле события**.
	• В поле события вы можете указать одно из следующих значений:
	  • Поле `Extra`.
	  • Значение из поля `Extra` в следующем формате:
	  `Extra.<field name>`
	  Например, `Extra.app`.
	  Вам нужно указать значение вручную.
	  • Значение из массива, записанного в поле `Extra`, в следующем формате:
	  `Extra.<field name>.<array element>`
	  Например, `Extra.array.0`.
	  Нумерация значений в массиве начинается с 0. Вам нужно указать значение вручную. Для работы со значением из поля `Extra` на глубине 3 и ниже требуется использовать кавычки ``, например `` `Extra.lev1.lev2.lev3` ``.
	• Оператор – =.
	• Правый операнд – **константа**.
	• Значение – значение, по которому требуется фильтровать события.
	
	Последовательность условий, указанных в фильтре селектора корреляционного правила, имеет значение и влияет на производительность системы. Мы рекомендуем на первое место в фильтре селектора ставить наиболее уникальный критерий отбора.
	
	Рассмотрим два примера фильтров селектора, осуществляющих выборку событий успешной аутентификации в Microsoft Windows.
	
	Фильтр селектора 1:
	
	Условие 1 – `DeviceProduct = Microsoft Windows`.
	
	Условие 2 – `DeviceEventClassID =  4624`.
	
	Фильтр селектора 2:
	
	Условие 1 – `DeviceEventClassID = 4624`.
	
	Условие 2 – `DeviceProduct = Microsoft Windows`.
	
	Последовательность условий, указанная в фильтре селектора 2, является более предпочтительной, так как показывает меньшую нагрузку на систему.

На вкладке **Локальные переменные** вы можете добавить переменные, которые будут действовать в пределах правила корреляции. Для добавления переменной нажмите на кнопку **+ Добавить**, после чего укажите переменную и ее значение. Вы можете добавить несколько переменных и удалить переменные. Для удаления переменной установите рядом с ней флажок и нажмите на кнопку **Удалить**.

В селекторе корреляционного правила могут быть использованы регулярные выражения, соответствующие стандарту RE2. Применение регулярных выражений в корреляционных правилах создает большую нагрузку в сравнении с другими операциями. При разработке корреляционных правил мы рекомендуем ограничить использование регулярных выражений до необходимого минимума и применять другие доступные операции.

Для использования регулярного выражения вам нужно применить оператор сравнения `match`. Регулярное выражение должно быть размещено в константе. Применение capture-групп в регулярных выражениях не обязательно. Для срабатывания корреляционного правила текст поля, сопоставляемый с regexp, должен полностью совпасть с регулярным выражением.

Для ознакомления с синтаксисом и примерами корреляционных правил, в селекторах которых есть регулярные выражения, вы можете использовать следующие правила, поставляемые с Kaspersky SIEM Cloud:

- R105_04_Подозрительные PowerShell-команды. Подозрение на обфускацию.
- R333_Подозрительное создание файлов в директории автозапуска.

Вкладка Действия

Эта вкладка используется для настройки триггеров правила корреляции. Вы можете настроить триггеры на следующих вкладках:

- **На первом срабатывании правила** – триггер срабатывает, когда контейнер регистрирует первое в течение срока своей жизни срабатывание селектора.
- **На последующих срабатываниях правила** – триггер срабатывает, когда контейнер регистрирует в течение срока своей жизни второе и последующие срабатывания селектора.
- **На каждом срабатывании правила** – триггер срабатывает каждый раз, когда контейнер регистрирует срабатывание селектора.
- **По истечении времени жизни контейнера** – триггер срабатывает по истечении времени жизни контейнера и используется в связке с селектором, в параметрах которого включен переключатель **Обнуление**. Таким образом, триггер срабатывает, если в течение указанного времени жизни ситуация, обнаруженная правилом корреляции, не разрешается.

Доступные параметры триггеров описаны в таблице ниже.

Параметр	Описание

Обогащение

Правила обогащения для изменения значений полей корреляционных событий. Правила обогащения хранятся в правиле корреляции, в котором они были созданы. Для создания правила обогащения нажмите на кнопку **+ Добавить обогащение**.

Доступные параметры правила обогащения:

- **Исходный тип** – тип обогащения. При выборе определенных типов обогащения могут стать доступны дополнительные параметры, для которых вам нужно указать значения.
  Доступные типы обогащения:

  - **константа**

    Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения описаны в таблице ниже.

    Параметры типа обогащения "константа"

Параметр	Описание
Константа	Значение, которое требуется добавить в поле события. Максимальная длина значения – до 255 символов в кодировке Unicode. Если оставить поле пустым, существующее значение поля события будет удалено.
Целевое поле	Поле события, в которое требуется поместить данные.

    Если вы используете функции обогащения событий для полей расширенной схемы с типом `Строка`, `Число` или `Число с плавающей точкой` с помощью константы, в поле будет добавлена константа.

    Если вы используете функции обогащения событий для полей расширенной схемы с типом `Массив строк`, `Массив чисел` или `Массив чисел с плавающей точкой` с помощью константы, константа будет добавлена к элементам массива.

  - **словарь**

    Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**. Параметры этого типа обогащения описаны в таблице ниже.

    Параметры типа обогащения "словарь"

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.

    Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **словарь**, а в параметре **Ключевые поля обогащения** указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку в соответствии с правилами сериализации одного значения в формате TSV.

    Пример. В параметре **Ключевые поля обогащения** используется поле расширенной схемы `SA.StringArrayOne`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`. В качестве ключа в словарь будут переданы значения `['a','b','c']`.

    Если в параметре **Ключевые поля обогащения** используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом `|`.

    Пример. В параметре **Ключевые поля обогащения** используется поле расширенной схемы `SA.StringArrayOne` и строковое поле `Code`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`, а строковое поле `Code` содержит последовательность символов `myCode`. В качестве ключа в словарь будут переданы значения `['a','b','c']|myCode`.

  - **таблица**

    Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**. Параметры этого типа обогащения описаны в таблице ниже.

    Параметры типа обогащения "таблица"

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.
Сопоставление	Поля событий для передачи данных: • **Поле словаря** – поля словаря, из которых будут передаваться данные. Доступные поля зависят от выбранного ресурса словаря. • **Поле KUMA** – поля событий, в которые будут передаваться данные. Для выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** вы можете задать название для помещаемых данных.

    Первое поле в таблице (**Поле словаря**) считается ключом, с которым будут сопоставляться поля, выбранные из события в качестве ключевых (**Поле KUMA**). В качестве ключа в **Поле словаря** вам нужно выбрать индикатор компрометации, по которому будет осуществляться обогащение, например IP-адрес, URL-адрес или хеш. В правиле необходимо выбрать поле события, соответствующее выбранному индикатору в поле словаря.

    Если вы хотите выбрать несколько ключевых полей, вы можете указать их через разделитель `|` (при указании через веб-интерфейс или импорте через CSV-файл), например `<IP-адрес>|<имя пользователя>`.

Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить**. Для удаления строки таблицы нажмите на крестик ✕.

- **событие**

  Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Целевое поле	Поле события Kaspersky SIEM Cloud, в которое требуется поместить данные.
Исходное поле	Поле события, значение которого будет записано в целевое поле.

Если вы хотите создать правило для изменения исходных данных перед записью в поля событий Kaspersky SIEM Cloud, в блоке параметров **Преобразование** нажмите на кнопку **+ Добавить преобразование**. В раскрывающемся списке **Тип** выберите нужный тип преобразования. Вы можете добавить несколько преобразований по кнопке **+ Добавить преобразование**. Чтобы удалить добавленное преобразование, нажмите рядом с ним на значок корзины.

Доступные преобразования

Преобразования – это изменения, которые применяются к значению перед записью в поле события.

Вы можете выбрать в раскрывающемся списке один из следующих типов преобразования:

- **entropy** – используется для преобразования значения исходного поля с помощью функции вычисления информационной энтропии и помещения результата преобразования в целевое поле типа `float`. Результатом преобразования будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например, когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.
- **lower** – используется для перевода всех символов значения в нижний регистр.
- **upper** – используется для перевода всех символов значения в верхний регистр.
- **regexp** – используется для преобразования значения с помощью указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.
- **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
  - **Символы на замену** – последовательность символов, которую требуется заменить.
  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.
- **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` требуется выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.
- **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.
- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.
- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.
  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.
- Конвертация закодированных строк в текст:
  - **decodeHexString** – используется для конвертации HEX-строки в текст.
  - **decodeBase64String** – используется для конвертации Base64-строки в текст.
  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.
  - **unicodeUnescape** – используется для конвертации Unicode-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.

  Мы не рекомендуем использовать несколько дополнительных нормализаторов для последовательного преобразования одного и того же поля. Результат одного преобразования, выполненного дополнительным нормализатором, не используется как входные данные для следующего. В итоговое событие записывается значение, полученное в дополнительном нормализаторе, который первым выполнил обогащение этого поля.

- Преобразование формата IP-адреса в IPv4:
  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
- **hexToDecimal** – используется для преобразования числового значения, представленного в шестнадцатеричной системе счисления, в десятичный формат. Преобразование применяется к строковым или числовым полям, содержащим HEX-значения (включая префикс 0x, если он присутствует), и результат записывается в целевое поле события Kaspersky SIEM Cloud в виде целого числа.

  Результатом преобразования является число в десятичной системе, например исходное значение – 0x00FF, после преобразования – 255.

При использовании обогащения событий, у которых в качестве параметра **Тип источника данных** выбрано значение **событие**, а в качестве аргументов используются поля расширенной схемы событий, необходимо учесть следующие особенности:

- Если исходное поле расширенной схемы событий имеет тип `Массив строк`, а целевое поле расширенной схемы событий имеет тип `Строка`, значения будут размещены в целевом поле расширенной схемы событий в формате TSV.

  Пример: в поле расширенной схемы событий `SA.StringArray`, находятся значения `"string1"`, `"string2"`, `"string3"`. Выполняется операция обогащения событий. Результат выполнения операции обогащения событий заносится в поле расширенной схемы событий `DeviceCustomString1`. В поле расширенной схемы событий `DeviceCustomString1` будут находиться значения `["string1", "string2", "string3"]`.

- Если исходное и целевое поля расширенной схемы событий имеют тип `Массив строк`, значения целевого поля расширенной схемы событий будут дополнены значениями исходного поля расширенной схемы событий, а качестве символа-разделителя будет использован символ `","`.

  Пример: в поле расширенной схемы событий `SA.StringArrayOne`, находятся значения `["string1", "string2", "string3"]`, а в поле расширенной схемы событий `SA.StringArrayTwo` находятся значения `["string4", "string5", "string6"]`. Выполняется операция обогащения событий. Результат выполнения операции обогащения событий заносится в поле расширенной схемы событий `SA.StringArrayTwo`. В поле расширенной схемы событий `SA.StringArrayTwo` будут находиться значения `["string4", "string5", "string6", "string1", "string2", "string3"]`.

- **шаблон**

  Этот тип обогащения используется, если в поле события нужно записать значение, полученное при обработке шаблонов Go. Мы рекомендуем сопоставлять значение и размер поля. Параметры этого типа обогащения описаны в таблице ниже.

  Параметры типа обогащения "шаблон"

Параметр	Описание
Шаблон	Шаблон Go. Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт, например `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.
Целевое поле	Поле события, в которое требуется поместить данные.

  Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **шаблон**, целевым полем является поле с типом `Строка`, а исходным полем является поле расширенной схемы событий, содержащее массив строк, то в шаблоне может быть использован один из следующих примеров:

  - `{{.SA.StringArrayOne}}`
  - ```
    {{- range $index, $element := . SA.StringArrayOne -}}
    {{- if $index}}, {{end}}"{{$element}}"{{- end -}}
    ```

  Для преобразования в шаблоне данных поля массива в формат TSV требуется использовать функцию `toString`, например:

  ```
  template {{toString .SA.StringArray}}
  ```

Обязательный параметр.

- **Отладка** – переключатель, включающий логирование ресурса. По умолчанию этот переключатель выключен.
- **Теги**

Вы можете создать несколько правил обогащения, изменить порядок правил обогащения и удалить правила обогащения. Для изменения порядка правил обогащения используйте значки изменения порядка ⣿. Для удаления правила обогащения нажмите рядом с ним на значок удаления ✕.

В дальнейшую обработку	Флажок, включающий отправку корреляционных событий на *пост-обработку* – на внешнее обогащение вне корреляционного правила, для реагирования и в точки назначения. По умолчанию этот флажок снят.
В коррелятор	Флажок, включающий обработку созданного корреляционного события цепочкой правил текущего коррелятора. Это позволят достичь иерархической корреляции. По умолчанию этот флажок снят. Если вы устанавливаете флажки **В дальнейшую обработку** и **В коррелятор**, правило корреляции будет отправлено сначала на пост-обработку, а затем в селекторы текущего правила корреляции.
Не создавать алерт	Флажок, выключающий создание алертов при срабатывании правила корреляции. По умолчанию этот флажок снят. Если вы хотите, чтобы алерт не создавался при срабатывании правила корреляции, но корреляционное событие все-равно отправлялось в хранилище, установите флажки **В дальнейшую обработку** и **Не создавать алерт**. Если установлен только флажок **Не создавать алерт**, корреляционное событие не будет сохраняться в хранилище.
  ```

Изменение категорий	Правила категоризации для изменения категорий активов, указанных в событии. С помощью правил категоризации вы можете привязывать и отвязывать от активов только реактивные категории. Для создания правила категоризации нажмите на кнопку **+ Добавить категоризацию**.
	Доступные параметры правила категоризации:
	• **Действие** – операция, выполняемая над категорией:
	  • **Добавить** – привязать категорию к активу.
	  • **Удалить** – отвязать категорию от актива.
	  Обязательный параметр.
	• **Поле события** – поле события, содержащее актив, над которым будет выполнена операция.
	  Обязательный параметр.
	• **Идентификатор категории** – категория, над которой будет совершена операция.
	  Обязательный параметр.
	Вы можете создать несколько правил категоризации, изменить порядок правил категоризации и удалить правила категоризации. Для изменения порядка правил категоризации используйте значки изменения порядка ⣿. Для удаления правила категоризации нажмите рядом с ним на значок удаления ✕.

Обновление активных листов	Операции с активными листами. Для создания операции с активным листом нажмите на кнопку **+ Добавить действие с активным листом**.
	Доступные параметры операции с активным листом:
	• **Название** – активный лист, с которым выполняется операция. Если вы хотите изменить параметры активного листа, нажмите рядом с ним на значок карандаша 🖉.
	  Обязательный параметр.
	• **Операция** – операция, которая выполняется с активным листом:
	  • **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению активного листа.
	  • **Установить** – записать значения указанных полей корреляционного события в активный лист, создав новую или обновив существующую запись активного листа. При обновлении записи активного листа данные объединяются, и только указанные поля перезаписываются.
	  • **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.
	  • **Удалить** – удалить запись из активного листа.
	  Обязательный параметр.
	• **Ключевые поля** – поля события, которые используются для создания записи активного листа. Указанные поля событий также используются в качестве ключа записи активного листа.
	  > Ключ записи активного листа зависит только от состава полей событий и не зависит от порядка их отображения в веб-интерфейсе Kaspersky SIEM Cloud.
	  Обязательный параметр.
	• **Сопоставление** – правила сопоставления полей активного листа с полями событий. Вы можете использовать правила сопоставления, если в раскрывающемся списке **Операция** вы выбрали значение **Получить** или **Установить**. Для создания правила сопоставления нажмите на кнопку **+ Добавить**.
	  Доступные параметры правила сопоставления:
	  • **Поле активного листа** – поле активного листа, которое сопоставляется с полем события. Поле не должно содержать специальные символы или только цифры.
	  • **Поле Kaspersky SIEM Cloud** – поле события, с которым сопоставляется поле активного листа.
	  • **Константа** – константа, которая назначается полю активного листа. Вам нужно указать константу, если в раскрывающемся списке **Операция** вы выбрали значение **Установить**.
	  Вы можете создать несколько правил сопоставления и удалить правила сопоставления. Для удаления правила сопоставления установите рядом с ним флажок и нажмите на кнопку **Удалить**.
	Вы можете создать несколько операций с активными листами, изменить порядок операций с активными листами и удалить операции с активными листами. Для изменения порядка операций с активными листами используйте значки изменения порядка ⣿. Для удаления операции с активным листом нажмите рядом с ней на значок удаления ✕.

Обновление контекстных таблиц	Операции с контекстными таблицами. Для создания операции с контекстной таблицей нажмите на кнопку **+ Добавить действие с контекстной таблицей**.
	Доступные параметры операции с контекстной таблицей:
	• **Название** – контекстная таблица, с которой выполняется операция. Если вы хотите изменить параметры контекстной таблицы, нажмите рядом с ней на значок карандаша. Обязательный параметр.
	• **Операция** – операция, которая выполняется с контекстной таблицей:
	  • **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению указанного поля контекстной таблицы. Операция используется только для полей с типом `Число` и `Число с плавающей точкой`.
	  • **Установить** – записать значения указанных полей корреляционного события в контекстную таблицу, создав новую или обновив существующую запись контекстной таблицы. При обновлении записи контекстной таблицы данные объединяются, и только указанные поля перезаписываются.
	  • **Объединить** – дописать значение поля корреляционного события, локальной переменной или константы к существующему значению поля контекстной таблицы.
	  • **Получить** – получить поля контекстной таблицы и записать значения указанных полей в корреляционное событие. Поля таблицы типа булево значение и список булевых значений исключаются из сопоставления, потому что в событии нет полей булева типа.
	  • **Удалить** – удалить запись из контекстной таблицы.
	  Обязательный параметр.
	• **Сопоставление** – правила сопоставления полей контекстной таблицы с полями событий или переменными. Вы можете использовать правила сопоставления, если в раскрывающемся списке **Операция** вы не выбрали значение **Удалить**. Для создания правила сопоставления нажмите на кнопку **+ Добавить**.
	Доступные параметры правила сопоставления:
	  • **Поле контекстной таблицы** – поле контекстной таблицы, которое сопоставляется с полем события. Вы не можете указать поле контекстной таблицы, которое уже используется в сопоставлении. Вы можете указать табуляцию, специальные символы или только цифры. Максимальное длина названия поля контекстной таблицы составляет 128 символов. Название поля контекстной таблицы не может начинаться с нижнего подчеркивания.
	  • **Поле Kaspersky SIEM Cloud** – поле события или локальная переменная, с которой сопоставляется поле контекстной таблицы.
	  • **Константа** – константа, которая назначается полю контекстной таблицы. Вам нужно указать константу, если в раскрывающемся списке **Операция** вы выбрали значение **Установить**, **Объединить** или **Сложить**. Максимальное длина константы составляет 1024 символа.
	  Вы можете создать несколько правил сопоставления и удалить правила сопоставления. Для удаления правила сопоставления установите рядом с ним флажок и нажмите на кнопку **Удалить**.
	Вы можете создать несколько операций с контекстными таблицами, изменить порядок операций с контекстными таблицами и удалить операции с контекстными таблицами. Для изменения порядка операций с контекстными таблицами используйте значки изменения порядка. Для удаления операции с контекстной таблицей нажмите рядом с ней на значок удаления.

Вкладка Корреляторы

Эта вкладка отображается только при изменении параметров созданного правила корреляции и используется для привязки правила корреляции к коррелятору.

Для привязки правила корреляции к коррелятору нажмите на кнопку **Привязать к сервису** → **Привязать к коррелятору**, в открывшемся окне укажите один или несколько корреляторов и нажмите на кнопку **ОК**. Правило корреляции будет привязано к указанным корреляторам и добавлено последним в очередь для выполнения в параметрах корреляторов. Если вы хотите изменить позицию правила корреляции в очереди для выполнения, перейдите в раздел **Ресурсы** → **Коррелятор**, нажмите на коррелятор, в открывшемся окне перейдите в раздел **Корреляция**, установите флажок рядом с правилом корреляции и измените позицию правила корреляции, нажимая на кнопки **Поднять** и **Опустить**.

Вы можете добавить несколько корреляторов и удалить корреляторы. Для этого нужно установить флажок рядом с коррелятором, нажать на кнопку **Удалить** и подтвердить удаление.

Правило корреляции, тип simple

Правила корреляции с типом **simple** используются для определения простых последовательностей событий. Доступные параметры правила корреляции с типом **simple** описаны в таблицах ниже.

Для правил корреляции установлено ограничение частоты срабатывания – одно срабатывание в секунду. Изменить частоту срабатывания правила невозможно.

По сравнению с моделью данных нормализованного события некоторые поля корреляционного события, образованного по правилу корреляции **simple**, могут отличаться (см. таблицу ниже).

Название поля корреляционного события	Описание
StartTime	Дата и время создания базового события (timestamp), от которого было образовано корреляционное событие.
EndTime	Дата и время создания базового события (timestamp), от которого было образовано корреляционное событие.

Вкладка Общие

Эта вкладка используется для указания основных параметров правила корреляции.

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип правила корреляции – **simple**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Наследуемые поля	Поля событий, по которым отбираются события. Если срабатывает селектор, указанный на вкладке **Селекторы**, отобранные поля событий копируются в корреляционное событие.
Уровень важности	Базовый коэффициент, используемый для определения уровня важности правила корреляции: • **Критический**. • **Высокий**. • **Средний**. • **Низкий** – это значение выбрано по умолчанию.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.
Техники MITRE	Загруженные техники MITRE ATT&CK для анализа состояния покрытия безопасности с помощью матрицы MITRE ATT&CK.

Вкладка Селекторы

Эта вкладка используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Для селектора доступны вкладки **Параметры** и **Локальные переменные**.

Параметры, доступные на вкладке **Параметры**, описаны в таблице ниже.

Параметр	Описание
Фильтр	Фильтр, указывающий критерии определения событий, при получении которых будет срабатывать селектор. Вы можете выбрать существующий фильтр или создать новый фильтр. Для создания нового фильтра выберите значение **Создать**. Если вы хотите изменить параметры существующего фильтра, нажмите рядом с ним на значок карандаша. Если вы будете использовать фильтр в других правилах корреляции, вам нужно сохранять его как отдельный ресурс. **Как создать фильтр?** Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. Выберите режим создания фильтра: **Конструктор** или **Код**. При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра. 5. Если вы выбрали вариант **Конструктор**, выполните следующие действия: a. В раскрывающемся списке выберите логический оператор: • **И** – отбирает события, которые соответствуют всем указанным условиям. • **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий. • **НЕ** – отбирает события, которые не соответствуют всем указанным условиям. b. Нажмите на кнопку **Добавить условие**. c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра. **Операнды фильтров** • **Поля событий** – поле события, которое требуется использовать как операнд фильтра. • **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**. Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра. • **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – словарь, который требуется использовать. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря. • **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события. • **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать. • **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы. • **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда. • **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда. • **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.

Параметр	Описание

	• **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
	  • **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
	  • **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
	  • **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
	• **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константа, которую требуется присвоить операнду.
	• **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
	Операторы фильтров
	• **=** – левый операнд равен правому операнду.
	• **<** – левый операнд меньше правого операнда.
	• **<=** – левый операнд меньше или равен правому операнду.
	• **>** – левый операнд больше правого операнда.
	• **>=** – левый операнд больше или равен правому операнду.
	• **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
	• **contains** – левый операнд содержит значения правого операнда.
	• **startsWith** – левый операнд начинается с одного из значений правого операнда.
	• **endsWith** – левый операнд заканчивается одним из значений правого операнда.
	• **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
	• **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).
	Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.
	Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
	• **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
	Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
	• **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
	• **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
	• **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
	• **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
	• **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись.
	• **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.
	Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.
	Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.
	e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.
	Вы можете добавить несколько групп условий.
	6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.
	В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.
	7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕.
	8. Нажмите **Сохранить**.

Параметр	Описание

	Фильтрация по данным из поля события Extra
	Условия для фильтров по данным из поля события `Extra`:
	• Условие – **Если**.
	• Левый операнд – **поле события**.
	• В поле события вы можете указать одно из следующих значений:
	  • Поле `Extra`.
	  • Значение из поля `Extra` в следующем формате:
	  `Extra.<field name>`
	  Например, `Extra.app`.
	  Вам нужно указать значение вручную.
	  • Значение из массива, записанного в поле `Extra`, в следующем формате:
	  `Extra.<field name>.<array element>`
	  Например, `Extra.array.0`.
	  Нумерация значений в массиве начинается с 0. Вам нужно указать значение вручную. Для работы со значением из поля `Extra` на глубине 3 и ниже требуется использовать кавычки ``, например `` `Extra.lev1.lev2.lev3` ``.
	• Оператор – =.
	• Правый операнд – **константа**.
	• Значение – значение, по которому требуется фильтровать события.
	Последовательность условий, указанных в фильтре селектора корреляционного правила, имеет значение и влияет на производительность системы. Мы рекомендуем на первое место в фильтре селектора ставить наиболее уникальный критерий отбора.
	Рассмотрим два примера фильтров селектора, осуществляющих выборку событий успешной аутентификации в Microsoft Windows.
	Фильтр селектора 1:
	Условие 1 – `DeviceProduct = Microsoft Windows`.
	Условие 2 – `DeviceEventClassID =  4624`.
	Фильтр селектора 2:
	Условие 1 – `DeviceEventClassID = 4624`.
	Условие 2 – `DeviceProduct = Microsoft Windows`.
	Последовательность условий, указанная в фильтре селектора 2, является более предпочтительной, так как показывает меньшую нагрузку на систему.

На вкладке **Локальные переменные** вы можете добавить переменные, которые будут действовать в пределах правила корреляции. Для добавления переменной нажмите на кнопку **+ Добавить**, после чего укажите переменную и ее значение. Вы можете добавить несколько переменных и удалить переменные. Для удаления переменной установите рядом с ней флажок и нажмите на кнопку **Удалить**.

Вкладка Действия

Эта вкладка используется для настройки триггера правила корреляции. В правиле корреляции с типом **simple** может быть только один триггер, который срабатывает каждый раз, когда контейнер регистрирует срабатывание селектора. Доступные параметры триггера описаны в таблице ниже.

Параметр	Описание

Обогащение

Правила обогащения для изменения значений полей корреляционных событий. Правила обогащения хранятся в правиле корреляции, в котором они были созданы. Для создания правила обогащения нажмите на кнопку **+ Добавить обогащение**.

Доступные параметры правила обогащения:

- **Исходный тип** – тип обогащения. При выборе определенных типов обогащения могут стать доступны дополнительные параметры, для которых вам нужно указать значения.
  Доступные типы обогащения:

  - **константа**

    Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения описаны в таблице ниже.

    Параметры типа обогащения "константа"

Параметр	Описание
Константа	Значение, которое требуется добавить в поле события. Максимальная длина значения – до 255 символов в кодировке Unicode. Если оставить поле пустым, существующее значение поля события будет удалено.
Целевое поле	Поле события, в которое требуется поместить данные.

    Если вы используете функции обогащения событий для полей расширенной схемы с типом `Строка`, `Число` или `Число с плавающей точкой` с помощью константы, в поле будет добавлена константа.

    Если вы используете функции обогащения событий для полей расширенной схемы с типом `Массив строк`, `Массив чисел` или `Массив чисел с плавающей точкой` с помощью константы, константа будет добавлена к элементам массива.

  - **словарь**

    Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**. Параметры этого типа обогащения описаны в таблице ниже.

    Параметры типа обогащения "словарь"

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.

    Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **словарь**, а в параметре **Ключевые поля обогащения** указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку в соответствии с правилами сериализации одного значения в формате TSV.

    Пример. В параметре **Ключевые поля обогащения** используется поле расширенной схемы `SA.StringArrayOne`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`. В качестве ключа в словарь будут переданы значения `['a','b','c']`.

    Если в параметре **Ключевые поля обогащения** используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом `|`.

    Пример. В параметре **Ключевые поля обогащения** используется поле расширенной схемы `SA.StringArrayOne` и строковое поле `Code`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`, а строковое поле `Code` содержит последовательность символов `myCode`. В качестве ключа в словарь будут переданы значения `['a','b','c']|myCode`.

  - **таблица**

    Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**. Параметры этого типа обогащения описаны в таблице ниже.

    Параметры типа обогащения "таблица"

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.
Сопоставление	Поля событий для передачи данных: • **Поле словаря** – поля словаря, из которых будут передаваться данные. Доступные поля зависят от выбранного ресурса словаря. • **Поле KUMA** – поля событий, в которые будут передаваться данные. Для выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** вы можете задать название для помещаемых данных.

    Первое поле в таблице (**Поле словаря**) считается ключом, с которым будут сопоставляться поля, выбранные из события в качестве ключевых (**Поле KUMA**). В качестве ключа в **Поле словаря** вам нужно выбрать индикатор компрометации, по которому будет осуществляться обогащение, например IP-адрес, URL-адрес или хеш. В правиле необходимо выбрать поле события, соответствующее выбранному индикатору в поле словаря.

    Если вы хотите выбрать несколько ключевых полей, вы можете указать их через разделитель `|` (при указании через веб-интерфейс или импорте через CSV-файл), например `<IP-адрес>|<имя пользователя>`.

Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить**. Для удаления строки таблицы нажмите на крестик ✕.

- **событие**

  Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Доступные параметры типа обогащения описаны в таблице ниже.

  Доступные параметры типа обогащения

Параметр	Описание
Целевое поле	Поле события Kaspersky SIEM Cloud, в которое требуется поместить данные.
Исходное поле	Поле события, значение которого будет записано в целевое поле.

Если вы хотите создать правило для изменения исходных данных перед записью в поля событий Kaspersky SIEM Cloud, в блоке параметров **Преобразование** нажмите на кнопку **+ Добавить преобразование**. В раскрывающемся списке **Тип** выберите нужный тип преобразования. Вы можете добавить несколько преобразований по кнопке **+ Добавить преобразование**. Чтобы удалить добавленное преобразование, нажмите рядом с ним на значок корзины.

Доступные преобразования

Преобразования – это изменения, которые применяются к значению перед записью в поле события.

Вы можете выбрать в раскрывающемся списке один из следующих типов преобразования:

- **entropy** – используется для преобразования значения исходного поля с помощью функции вычисления информационной энтропии и помещения результата преобразования в целевое поле типа `float`. Результатом преобразования будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например, когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.
- **lower** – используется для перевода всех символов значения в нижний регистр.
- **upper** – используется для перевода всех символов значения в верхний регистр.
- **regexp** – используется для преобразования значения с помощью указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.
- **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
  - **Символы на замену** – последовательность символов, которую требуется заменить.
  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.
- **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` требуется выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.
- **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.
- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.
- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.
  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.
- Конвертация закодированных строк в текст:
  - **decodeHexString** – используется для конвертации HEX-строки в текст.
  - **decodeBase64String** – используется для конвертации Base64-строки в текст.
  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.
  - **unicodeUnescape** – используется для конвертации Unicode-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.

  Мы не рекомендуем использовать несколько дополнительных нормализаторов для последовательного преобразования одного и того же поля. Результат одного преобразования, выполненного дополнительным нормализатором, не используется как входные данные для следующего. В итоговое событие записывается значение, полученное в дополнительном нормализаторе, который первым выполнил обогащение этого поля.

- Преобразование формата IP-адреса в IPv4:
  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.
- **hexToDecimal** – используется для преобразования числового значения, представленного в шестнадцатеричной системе счисления, в десятичный формат. Преобразование применяется к строковым или числовым полям, содержащим HEX-значения (включая префикс 0x, если он присутствует), и результат записывается в целевое поле события Kaspersky SIEM Cloud в виде целого числа.

  Результатом преобразования является число в десятичной системе, например исходное значение – 0x00FF, после преобразования – 255.

При использовании обогащения событий, у которых в качестве параметра **Тип источника данных** выбрано значение **событие**, а в качестве аргументов используются поля расширенной схемы событий, необходимо учесть следующие особенности:

- Если исходное поле расширенной схемы событий имеет тип `Массив строк`, а целевое поле расширенной схемы событий имеет тип `Строка`, значения будут размещены в целевом поле расширенной схемы событий в формате TSV.

  Пример: в поле расширенной схемы событий `SA.StringArray`, находятся значения `"string1"`, `"string2"`, `"string3"`. Выполняется операция обогащения событий. Результат выполнения операции обогащения событий заносится в поле расширенной схемы событий `DeviceCustomString1`. В поле расширенной схемы событий `DeviceCustomString1` будут находиться значения `["string1", "string2", "string3"]`.

- Если исходное и целевое поля расширенной схемы событий имеют тип `Массив строк`, значения целевого поля расширенной схемы событий будут дополнены значениями исходного поля расширенной схемы событий, а качестве символа-разделителя будет использован символ `","`.

  Пример: в поле расширенной схемы событий `SA.StringArrayOne`, находятся значения `["string1", "string2", "string3"]`, а в поле расширенной схемы событий `SA.StringArrayTwo` находятся значения `["string4", "string5", "string6"]`. Выполняется операция обогащения событий. Результат выполнения операции обогащения событий заносится в поле расширенной схемы событий `SA.StringArrayTwo`. В поле расширенной схемы событий `SA.StringArrayTwo` будут находиться значения `["string4", "string5", "string6", "string1", "string2", "string3"]`.

- **шаблон**

  Этот тип обогащения используется, если в поле события нужно записать значение, полученное при обработке шаблонов Go. Мы рекомендуем сопоставлять значение и размер поля. Параметры этого типа обогащения описаны в таблице ниже.

  Параметры типа обогащения "шаблон"

Параметр	Описание
Шаблон	Шаблон Go. Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт, например `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.
Целевое поле	Поле события, в которое требуется поместить данные.

  Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **шаблон**, целевым полем является поле с типом `Строка`, а исходным полем является поле расширенной схемы событий, содержащее массив строк, то в шаблоне может быть использован один из следующих примеров:

  - `{{.SA.StringArrayOne}}`
  - ```
    {{- range $index, $element := . SA.StringArrayOne -}}
    {{- if $index}}, {{end}}"{{$element}}"{{- end -}}
    ```

  Для преобразования в шаблоне данных поля массива в формат TSV требуется использовать функцию `toString`, например:

  ```
  template {{toString .SA.StringArray}}
  ```

Обязательный параметр.

- **Отладка** – переключатель, включающий логирование ресурса. По умолчанию этот переключатель выключен.
- **Теги**

Вы можете создать несколько правил обогащения, изменить порядок правил обогащения и удалить правила обогащения. Для изменения порядка правил обогащения используйте значки изменения порядка ⣿. Для удаления правила обогащения нажмите рядом с ним на значок удаления ✕.

В дальнейшую обработку	Флажок, включающий отправку корреляционных событий на *пост-обработку* – на внешнее обогащение вне корреляционного правила, для реагирования и в точки назначения. По умолчанию этот флажок снят.
В коррелятор	Флажок, включающий обработку созданного корреляционного события цепочкой правил текущего коррелятора. Это позволят достичь иерархической корреляции. По умолчанию этот флажок снят. Если вы устанавливаете флажки **В дальнейшую обработку** и **В коррелятор**, правило корреляции будет отправлено сначала на пост-обработку, а затем в селекторы текущего правила корреляции.
Не создавать алерт	Флажок, выключающий создание алертов при срабатывании правила корреляции. По умолчанию этот флажок снят. Если вы хотите, чтобы алерт не создавался при срабатывании правила корреляции, но корреляционное событие все-равно отправлялось в хранилище, установите флажки **В дальнейшую обработку** и **Не создавать алерт**. Если установлен только флажок **Не создавать алерт**, корреляционное событие не будет сохраняться в хранилище.
  ```

Изменение категорий	Правила категоризации для изменения категорий активов, указанных в событии. С помощью правил категоризации вы можете привязывать и отвязывать от активов только реактивные категории. Для создания правила категоризации нажмите на кнопку **+ Добавить категоризацию**.
	Доступные параметры правила категоризации:
	• **Действие** – операция, выполняемая над категорией:
	  • **Добавить** – привязать категорию к активу.
	  • **Удалить** – отвязать категорию от актива.
	  Обязательный параметр.
	• **Поле события** – поле события, содержащее актив, над которым будет выполнена операция.
	  Обязательный параметр.
	• **Идентификатор категории** – категория, над которой будет совершена операция.
	  Обязательный параметр.
	Вы можете создать несколько правил категоризации, изменить порядок правил категоризации и удалить правила категоризации. Для изменения порядка правил категоризации используйте значки изменения порядка ⣿. Для удаления правила категоризации нажмите рядом с ним на значок удаления ✕.

Обновление активных листов	Операции с активными листами. Для создания операции с активным листом нажмите на кнопку **+ Добавить действие с активным листом**.
	Доступные параметры операции с активным листом:
	• **Название** – активный лист, с которым выполняется операция. Если вы хотите изменить параметры активного листа, нажмите рядом с ним на значок карандаша 🖉.
	  Обязательный параметр.
	• **Операция** – операция, которая выполняется с активным листом:
	  • **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению активного листа.
	  • **Установить** – записать значения указанных полей корреляционного события в активный лист, создав новую или обновив существующую запись активного листа. При обновлении записи активного листа данные объединяются, и только указанные поля перезаписываются.
	  • **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.
	  • **Удалить** – удалить запись из активного листа.
	  Обязательный параметр.
	• **Ключевые поля** – поля события, которые используются для создания записи активного листа. Указанные поля событий также используются в качестве ключа записи активного листа.
	  > Ключ записи активного листа зависит только от состава полей событий и не зависит от порядка их отображения в веб-интерфейсе Kaspersky SIEM Cloud.
	  Обязательный параметр.
	• **Сопоставление** – правила сопоставления полей активного листа с полями событий. Вы можете использовать правила сопоставления, если в раскрывающемся списке **Операция** вы выбрали значение **Получить** или **Установить**. Для создания правила сопоставления нажмите на кнопку **+ Добавить**.
	  Доступные параметры правила сопоставления:
	  • **Поле активного листа** – поле активного листа, которое сопоставляется с полем события. Поле не должно содержать специальные символы или только цифры.
	  • **Поле Kaspersky SIEM Cloud** – поле события, с которым сопоставляется поле активного листа.
	  • **Константа** – константа, которая назначается полю активного листа. Вам нужно указать константу, если в раскрывающемся списке **Операция** вы выбрали значение **Установить**.
	  Вы можете создать несколько правил сопоставления и удалить правила сопоставления. Для удаления правила сопоставления установите рядом с ним флажок и нажмите на кнопку **Удалить**.
	Вы можете создать несколько операций с активными листами, изменить порядок операций с активными листами и удалить операции с активными листами. Для изменения порядка операций с активными листами используйте значки изменения порядка ⣿. Для удаления операции с активным листом нажмите рядом с ней на значок удаления ✕.

Обновление контекстных таблиц	Операции с контекстными таблицами. Для создания операции с контекстной таблицей нажмите на кнопку **+ Добавить действие с контекстной таблицей**.
	Доступные параметры операции с контекстной таблицей:
	• **Название** – контекстная таблица, с которой выполняется операция. Если вы хотите изменить параметры контекстной таблицы, нажмите рядом с ней на значок карандаша. Обязательный параметр.
	• **Операция** – операция, которая выполняется с контекстной таблицей:
	  • **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению указанного поля контекстной таблицы. Операция используется только для полей с типом `Число` и `Число с плавающей точкой`.
	  • **Установить** – записать значения указанных полей корреляционного события в контекстную таблицу, создав новую или обновив существующую запись контекстной таблицы. При обновлении записи контекстной таблицы данные объединяются, и только указанные поля перезаписываются.
	  • **Объединить** – дописать значение поля корреляционного события, локальной переменной или константы к существующему значению поля контекстной таблицы.
	  • **Получить** – получить поля контекстной таблицы и записать значения указанных полей в корреляционное событие. Поля таблицы типа булево значение и список булевых значений исключаются из сопоставления, потому что в событии нет полей булева типа.
	  • **Удалить** – удалить запись из контекстной таблицы.
	  Обязательный параметр.
	• **Сопоставление** – правила сопоставления полей контекстной таблицы с полями событий или переменными. Вы можете использовать правила сопоставления, если в раскрывающемся списке **Операция** вы не выбрали значение **Удалить**. Для создания правила сопоставления нажмите на кнопку **+ Добавить**.
	Доступные параметры правила сопоставления:
	  • **Поле контекстной таблицы** – поле контекстной таблицы, которое сопоставляется с полем события. Вы не можете указать поле контекстной таблицы, которое уже используется в сопоставлении. Вы можете указать табуляцию, специальные символы или только цифры. Максимальное длина названия поля контекстной таблицы составляет 128 символов. Название поля контекстной таблицы не может начинаться с нижнего подчеркивания.
	  • **Поле Kaspersky SIEM Cloud** – поле события или локальная переменная, с которой сопоставляется поле контекстной таблицы.
	  • **Константа** – константа, которая назначается полю контекстной таблицы. Вам нужно указать константу, если в раскрывающемся списке **Операция** вы выбрали значение **Установить**, **Объединить** или **Сложить**. Максимальное длина константы составляет 1024 символа.
	  Вы можете создать несколько правил сопоставления и удалить правила сопоставления. Для удаления правила сопоставления установите рядом с ним флажок и нажмите на кнопку **Удалить**.
	Вы можете создать несколько операций с контекстными таблицами, изменить порядок операций с контекстными таблицами и удалить операции с контекстными таблицами. Для изменения порядка операций с контекстными таблицами используйте значки изменения порядка. Для удаления операции с контекстной таблицей нажмите рядом с ней на значок удаления.

Вкладка Корреляторы

Эта вкладка отображается только при изменении параметров созданного правила корреляции и используется для привязки правила корреляции к коррелятору.

Для привязки правила корреляции к коррелятору нажмите на кнопку **Привязать к сервису** → **Привязать к коррелятору**, в открывшемся окне укажите один или несколько корреляторов и нажмите на кнопку **ОК**. Правило корреляции будет привязано к указанным корреляторам и добавлено последним в очередь для выполнения в параметрах корреляторов. Если вы хотите изменить позицию правила корреляции в очереди для выполнения, перейдите в раздел **Ресурсы** → **Коррелятор**, нажмите на коррелятор, в открывшемся окне перейдите в раздел **Корреляция**, установите флажок рядом с правилом корреляции и измените позицию правила корреляции, нажимая на кнопки **Поднять** и **Опустить**.

Вы можете добавить несколько корреляторов и удалить корреляторы. Для этого нужно установить флажок рядом с коррелятором, нажать на кнопку **Удалить** и подтвердить удаление.

Правило корреляции, тип operational

Правила корреляции с типом **operational** используются для работы с активными листами. Доступные параметры правила корреляции с типом **operational** описаны в таблицах ниже.

Для правил корреляции установлено ограничение частоты срабатывания – одно срабатывание в секунду. Изменить частоту срабатывания правила невозможно.

Вкладка Общие

Эта вкладка используется для указания основных параметров правила корреляции.

Параметр	Описание
Название	Уникальное имя ресурса. Максимальная длина имени составляет до 128 символов в кодировке Unicode. Обязательный параметр.
Тенант	Название тенанта, которому принадлежит ресурс. Обязательный параметр.
Тип	Тип правила корреляции – **operational**. Обязательный параметр.
Теги	Теги для поиска ресурса. Необязательный параметр.
Описание	Описание ресурса. Максимальная длина описания составляет до 4000 символов в кодировке Unicode.
Техники MITRE	Загруженные техники MITRE ATT&CK для анализа состояния покрытия безопасности с помощью матрицы MITRE ATT&CK.

Вкладка Селекторы

Эта вкладка используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Для селектора доступны вкладки **Параметры** и **Локальные переменные**.

Параметры, доступные на вкладке **Параметры**, описаны в таблице ниже.

Параметр	Описание
Фильтр	Фильтр, указывающий критерии определения событий, при получении которых будет срабатывать селектор. Вы можете выбрать существующий фильтр или создать новый фильтр. Для создания нового фильтра выберите значение **Создать**. Если вы хотите изменить параметры существующего фильтра, нажмите рядом с ним на значок карандаша. Если вы будете использовать фильтр в других правилах корреляции, вам нужно сохранять его как отдельный ресурс. **Как создать фильтр?** Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`. *Чтобы создать фильтр:* 1. В раскрывающемся списке **Фильтр** выберите **Создать**. 2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят. 3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode. 4. Выберите режим создания фильтра: **Конструктор** или **Код**. При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра. 5. Если вы выбрали вариант **Конструктор**, выполните следующие действия: a. В раскрывающемся списке выберите логический оператор: • **И** – отбирает события, которые соответствуют всем указанным условиям. • **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий. • **НЕ** – отбирает события, которые не соответствуют всем указанным условиям. b. Нажмите на кнопку **Добавить условие**. c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**. d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра. **Операнды фильтров** • **Поля событий** – поле события, которое требуется использовать как операнд фильтра. • **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**. Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра. • **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – словарь, который требуется использовать. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря. • **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события. • **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать. • **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы. • **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда. • **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда. • **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры: • **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**. • **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.

Параметр	Описание

	• **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
	  • **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
	  • **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
	  • **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
	• **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константа, которую требуется присвоить операнду.
	• **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
	  • **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
	Операторы фильтров
	• **=** – левый операнд равен правому операнду.
	• **<** – левый операнд меньше правого операнда.
	• **<=** – левый операнд меньше или равен правому операнду.
	• **>** – левый операнд больше правого операнда.
	• **>=** – левый операнд больше или равен правому операнду.
	• **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
	• **contains** – левый операнд содержит значения правого операнда.
	• **startsWith** – левый операнд начинается с одного из значений правого операнда.
	• **endsWith** – левый операнд заканчивается одним из значений правого операнда.
	• **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
	• **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).
	Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.
	Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
	• **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.
	Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
	• **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
	• **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
	• **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
	• **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
	• **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
	• **inContextTable** – присутствует ли в указанной контекстной таблице запись.
	• **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.
	Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.
	Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.
	e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.
	Вы можете добавить несколько групп условий.
	6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.
	В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.
	7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕.
	8. Нажмите **Сохранить**.

Параметр	Описание

	Фильтрация по данным из поля события Extra
	Условия для фильтров по данным из поля события `Extra`:
	• Условие – **Если**.
	• Левый операнд – **поле события**.
	• В поле события вы можете указать одно из следующих значений:
	  • Поле `Extra`.
	  • Значение из поля `Extra` в следующем формате:
	  `Extra.<field name>`
	  Например, `Extra.app`.
	  Вам нужно указать значение вручную.
	  • Значение из массива, записанного в поле `Extra`, в следующем формате:
	  `Extra.<field name>.<array element>`
	  Например, `Extra.array.0`.
	  Нумерация значений в массиве начинается с 0. Вам нужно указать значение вручную. Для работы со значением из поля `Extra` на глубине 3 и ниже требуется использовать кавычки ``, например `` `Extra.lev1.lev2.lev3` ``.
	• Оператор – =.
	• Правый операнд – **константа**.
	• Значение – значение, по которому требуется фильтровать события.
	Последовательность условий, указанных в фильтре селектора корреляционного правила, имеет значение и влияет на производительность системы. Мы рекомендуем на первое место в фильтре селектора ставить наиболее уникальный критерий отбора.
	Рассмотрим два примера фильтров селектора, осуществляющих выборку событий успешной аутентификации в Microsoft Windows.
	Фильтр селектора 1:
	Условие 1 – `DeviceProduct = Microsoft Windows`.
	Условие 2 – `DeviceEventClassID =  4624`.
	Фильтр селектора 2:
	Условие 1 – `DeviceEventClassID = 4624`.
	Условие 2 – `DeviceProduct = Microsoft Windows`.
	Последовательность условий, указанная в фильтре селектора 2, является более предпочтительной, так как показывает меньшую нагрузку на систему.

На вкладке **Локальные переменные** вы можете добавить переменные, которые будут действовать в пределах правила корреляции. Для добавления переменной нажмите на кнопку **+ Добавить**, после чего укажите переменную и ее значение. Вы можете добавить несколько переменных и удалить переменные. Для удаления переменной установите рядом с ней флажок и нажмите на кнопку **Удалить**.

Вкладка Действия

Эта вкладка используется для настройки триггера правила корреляции. В правиле корреляции с типом **operational** может быть только один триггер, который срабатывает каждый раз, когда контейнер регистрирует срабатывание селектора. Доступные параметры триггера описаны в таблице ниже.

Параметр	Описание

Обновление активных листов	Операции с активными листами. Для создания операции с активным листом нажмите на кнопку **+ Добавить действие с активным листом**.
	Доступные параметры операции с активным листом:
	• **Название** – активный лист, с которым выполняется операция. Если вы хотите изменить параметры активного листа, нажмите рядом с ним на значок карандаша.
	Обязательный параметр.
	• **Операция** – операция, которая выполняется с активным листом:
	  • **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению активного листа.
	  • **Установить** – записать значения указанных полей корреляционного события в активный лист, создав новую или обновив существующую запись активного листа. При обновлении записи активного листа данные объединяются, и только указанные поля перезаписываются.
	  • **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.
	  • **Удалить** – удалить запись из активного листа.
	  Обязательный параметр.
	• **Ключевые поля** – поля события, которые используются для создания записи активного листа. Указанные поля событий также используются в качестве ключа записи активного листа.
	  Ключ записи активного листа зависит только от состава полей событий и не зависит от порядка их отображения в веб-интерфейсе Kaspersky SIEM Cloud.
	  Обязательный параметр.
	• **Сопоставление** – правила сопоставления полей активного листа с полями событий. Вы можете использовать правила сопоставления, если в раскрывающемся списке **Операция** вы выбрали значение **Получить** или **Установить**. Для создания правила сопоставления нажмите на кнопку **+ Добавить**.
	  Доступные параметры правила сопоставления:
	  • **Поле активного листа** – поле активного листа, которое сопоставляется с полем события. Поле не должно содержать специальные символы или только цифры.
	  • **Поле Kaspersky SIEM Cloud** – поле события, с которым сопоставляется поле активного листа.
	  • **Константа** – константа, которая назначается полю активного листа. Вам нужно указать константу, если в раскрывающемся списке **Операция** вы выбрали значение **Установить**.
	  Вы можете создать несколько правил сопоставления и удалить правила сопоставления. Для удаления правила сопоставления установите рядом с ним флажок и нажмите на кнопку **Удалить**.
	Вы можете создать несколько операций с активными листами, изменить порядок операций с активными листами и удалить операции с активными листами. Для изменения порядка операций с активными листами используйте значки изменения порядка. Для удаления операции с активным листом нажмите рядом с ней на значок удаления.

Параметр	Описание
Обновление контекстных таблиц	Операции с контекстными таблицами. Для создания операции с контекстной таблицей нажмите на кнопку **+ Добавить действие с контекстной таблицей**. Доступные параметры операции с контекстной таблицей: • **Название** – контекстная таблица, с которой выполняется операция. Если вы хотите изменить параметры контекстной таблицы, нажмите рядом с ней на значок карандаша. Обязательный параметр. • **Операция** – операция, которая выполняется с контекстной таблицей: – **Сложить** – прибавить константу, значение поля корреляционного события или значение локальной переменной к значению указанного поля контекстной таблицы. Операция используется только для полей с типом `Число` и `Число с плавающей точкой`. – **Установить** – записать значения указанных полей корреляционного события в контекстную таблицу, создав новую или обновив существующую запись контекстной таблицы. При обновлении записи контекстной таблицы данные объединяются, и только указанные поля перезаписываются. – **Объединить** – дописать значение поля корреляционного события, локальной переменной или константы к существующему значению поля контекстной таблицы. – **Получить** – получить поля контекстной таблицы и записать значения указанных полей в корреляционное событие. Поля таблицы типа булево значение и список булевых значений исключаются из сопоставления, потому что в событии нет полей булева типа. – **Удалить** – удалить запись из контекстной таблицы. Обязательный параметр. • **Сопоставление** – правила сопоставления полей контекстной таблицы с полями событий или переменными. Вы можете использовать правила сопоставления, если в раскрывающемся списке **Операция** вы не выбрали значение **Удалить**. Для создания правила сопоставления нажмите на кнопку **+ Добавить**. Доступные параметры правила сопоставления: – **Поле контекстной таблицы** – поле контекстной таблицы, которое сопоставляется с полем события. Вы не можете указать поле контекстной таблицы, которое уже используется в сопоставлении. Вы можете указать табуляцию, специальные символы или только цифры. Максимальное длина названия поля контекстной таблицы составляет 128 символов. Название поля контекстной таблицы не может начинаться с нижнего подчеркивания. – **Поле Kaspersky SIEM Cloud** – поле события или локальная переменная, с которой сопоставляется поле контекстной таблицы. – **Константа** – константа, которая назначается полю контекстной таблицы. Вам нужно указать константу, если в раскрывающемся списке **Операция** вы выбрали значение **Установить**, **Объединить** или **Сложить**. Максимальное длина константы составляет 1024 символа. Вы можете создать несколько правил сопоставления и удалить правила сопоставления. Для удаления правила сопоставления установите рядом с ним флажок и нажмите на кнопку **Удалить**. Вы можете создать несколько операций с контекстными таблицами, изменить порядок операций с контекстными таблицами и удалить операции с контекстными таблицами. Для изменения порядка операций с контекстными таблицами используйте значки изменения порядка. Для удаления операции с контекстной таблицей нажмите рядом с ней на значок удаления.

Вкладка Корреляторы

Эта вкладка отображается только при изменении параметров созданного правила корреляции и используется для привязки правила корреляции к коррелятору.

Для привязки правила корреляции к коррелятору нажмите на кнопку **Привязать к сервису → Привязать к коррелятору**, в открывшемся окне укажите один или несколько коррелляторов и нажмите на кнопку **ОК**. Правило корреляции будет привязано к указанным корреляторам и добавлено последним в очередь для выполнения в параметрах корреляторов. Если вы хотите изменить позицию правила корреляции в очереди для выполнения, перейдите в раздел **Ресурсы → Коррелятор**, нажмите на коррелятор, в открывшемся окне перейдите в раздел **Корреляция**, установите флажок рядом с правилом корреляции и измените позицию правила корреляции, нажимая на кнопки **Поднять** и **Опустить**.

Вы можете добавить несколько корреляторов и удалить корреляторы. Для этого нужно установить флажок рядом с коррелятором, нажать на кнопку **Удалить** и подтвердить удаление.

Использование фильтров в правилах корреляции

С увеличением количества правил корреляции повышается сложность их поддержки. Вам может понадобиться внести изменения в параметры фильтров сразу нескольких правил корреляции. Например, вы можете добавить исключения для повышения точности детектирования или изменить условия фильтров при изменении параметров нормализации или при расширении покрытия правила.

Если вы вносите изменения в параметры фильтра каждого правила корреляции в отдельности и не сохраняете при этом фильтр в виде именованного ресурса, то со временем повышается риск допустить ошибку в фильтре. В результате в похожих правилах корреляции могут быть указаны разные параметры фильтров, так как одно из правил было обновлено, а другое нет. Такой подход также усложняет чтение условий фильтров, поскольку одно и то же условие в разных правилах может быть задано по-разному или несколько условий могут быть заданы в разном порядке.

Для решения этой проблемы рекомендуется использовать фильтры в виде именованных ресурсов, которые вы можете переиспользовать в разных правилах корреляции. В таком случае для применения новых параметров фильтров вам нужно внести изменения только в сам фильтр, и новые параметры будут применены автоматически ко всем правилам корреляции, в которых указан этот фильтр.

Как сохранить фильтр в виде ресурса

Чтобы создать фильтр в виде именованного ресурса,

выполните одно из следующих действий:

- Создайте фильтр в разделе **Ресурсы**.
- В окне создания или изменения ресурса при настройке фильтра установите флажок **Сохранить фильтр**, затем укажите название для нового фильтра. Например, при создании или изменении правила корреляции фильтр настраивается на вкладке **Селекторы**.

Фильтр будет создан и добавлен в список фильтров.

Примеры

Примеры использования фильтров в правилах корреляции:

- Есть правила корреляции, в условиях срабатывания которых указан один и тот же тип событий, например `DeviceEventClassID='4688'` (запуск процесса).

  Вы можете создать фильтр, указать в нем это условие и сохранить под соответствующим именем, например `4688: A new process has been created`. Затем этот фильтр можно использовать во всех правилах, срабатывание которых основано на этом типе событий.

- Вам нужно исключить из корреляционной логики легитимные события, например действия администраторов. При этом у всех администраторов имена учетных записей начинаются с `adm_`.

  Вы можете создать фильтр, указать в нем такое условие и сохранить под соответствующим именем, например `Exclusions: adm_`. Каждое из условий исключений вы можете сохранить в отдельный фильтр с префиксом `Exclusions:` в имени. В результате вы получите набор фильтров для исключений. Такой подход облегчает поддержку правил и анализ исключений.

Примеры часто используемых фильтров:

- Фильтры для типов источников событий (например, Windows, Linux).
- Фильтры для применения правил только на определенных хостах (например, хост контроллера домена) или учетных записях (например, сервисные учетные записи или пользователи определенного отдела).
- Фильтры для часто используемых исключений.
- Фильтры для определенных типов событий Kaspersky SIEM Cloud (например, базовых или корреляционных).
- Фильтры для конкретных событий (например, типов интерактивной аутентификации Windows).

Ограничение количества срабатываний правила корреляции

Если правило корреляции должно срабатывать ограниченное количество раз за определенный период, количество его срабатываний можно хранить в активном листе и использовать это значение при обработке правила. Например, нужно ограничить количество срабатываний правила корреляции десятью в сутки. Для этого в активном листе хранится счетчик срабатываний и для каждого правила и каждой даты используется отдельная запись. При срабатывании правила значение счетчика увеличивается на единицу, а после достижения значения 10 правило не должно срабатывать до начала следующего дня.

Настройка ограничения количества срабатываний правила корреляции состоит из следующих этапов:

1. Создание активного листа

Создайте активный лист, в котором будет храниться количество срабатываний правила корреляции.

1. В веб-интерфейсе перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные листы**.
2. Нажмите на кнопку **Создать**.
3. Укажите параметры активного листа:
   a. В поле **Название** укажите, например, `correlation_limits`.
   b. В раскрывающемся списке **Тенант** выберите нужный тенант.
   c. В поле **Срок жизни** укажите срок хранения записи активного листа.
4. При необходимости заполните поля **Теги** и **Описание**.
5. Нажмите на кнопку **Сохранить**.

Активный лист будет добавлен.

В качестве поля для хранения количества срабатываний используйте `_count`. Для записи активного листа задайте ключ, состоящий из названия правила корреляции и даты события (например `LimitRule_Example_2026-09-06`). Такой ключ позволяет хранить отдельный счетчик для каждого правила корреляции за каждый день.

❷ Настройка правила корреляции

1. Создайте или откройте параметры существующего правила корреляции типа **standard**.
2. На вкладке **Общие** укажите основные параметры правила, включая **Название**, **Тенант** и **Тип**.
3. На вкладке **Селекторы** настройте условия, по которым правило должно отбирать события.
4. Перейдите на вкладку **Действия**.
5. В блоке **Обновление активных листов** нажмите **+ Добавить действие с активным листом** и укажите следующие параметры:
   a. В поле **Название** выберите созданный ранее активный лист.
   b. В поле **Операция** выберите операцию, необходимую для работы со счетчиком:
      - **Получить** – получить текущее значение `_count`.
      - **Установить** – создать или обновить запись.
      - **Сложить** – увеличить значение счетчика.
6. Для обращения к одной записи активного листа используйте **Ключевые поля**. В них должны входить поля события, из которых формируется ключ записи: название правила корреляции и дата события.
7. В блоке параметров **Сопоставление** настройте соответствие поля `_count` и поля события, если оно нужно для выбранной операции.
8. Настройте обработку полученного значения `_count`:
   - Если записи за текущую дату нет, счетчик должен быть установлен в 1.
   - Если значение `_count` меньше 10, счетчик должен быть увеличен на 1, а правило должно сработать.
   - Если `_count` равен 10, правило не должно срабатывать.
9. Сохраните правило корреляции.

❸ Привязка активного листа и правила корреляции

Привяжите активный лист к правилу корреляции, а правило корреляции – к коррелятору.

1. Откройте созданное правило корреляции.
2. Перейдите на вкладку **Сервисы**.
3. Нажмите **Привязать к сервису** → **Привязать к коррелятору**.
4. В открывшемся окне выберите один или несколько корреляторов.
5. Нажмите на кнопку **OK**.

После привязки правило корреляции будет добавлено в очередь выполнения выбранного коррелятора. При необходимости его позицию в очереди можно изменить в разделе **Ресурсы** → **Корреляторы** → **[нужный коррелятор]** → **Корреляция**, используя кнопки **Поднять** и **Опустить**.

Убедитесь, что активный лист доступен для коррелятора, к которому привязано правило корреляции.

4 Проверка результата

Отправьте примеры событий, соответствующих условиям селектора правила корреляции, чтобы проверить количество срабатываний и значение `_count` в активном листе.

1. Отправьте первое событие.

   Убедитесь, что правило сработало, а в активном листе создана запись для текущей даты со значением `_count = 1`.

2. Последовательно отправьте еще восемь событий.

   Убедитесь, что правило продолжает срабатывать, а значение `_count` увеличивается до 9.

3. Отправьте десятое событие.

   Убедитесь, что правило сработало, а значение `_count` стало равно 10.

4. Отправьте еще одно событие, соответствующее условиям селектора.

   Убедитесь, что правило не сработало и значение `_count` осталось равным 10.

5. После наступления следующего дня отправьте событие, соответствующее условиям селектора.

   Убедитесь, что для новой даты используется отдельная запись активного листа и правило снова может сработать.

Чтобы просмотреть записи активного листа, перейдите в **Ресурсы** → **Активные листы** и выберите нужный активный лист. В открывшейся таблице отображаются **Ключ**, **Значение**, **Срок действия**, **Последнее обновление** и другие параметры записи.

Переменные в корреляторах

Если для покрытия каких-то сценариев обеспечения безопасности недостаточно отслеживания значений в полях событий, активных листах или словарях, вы можете воспользоваться глобальными и локальными *переменными*. С их помощью можно выполнять различные действия над поступающими в корреляторы значениями, реализуя сложную логику выявления угроз. Переменные можно объявить в коррелляторе (*глобальные переменные*) или в правиле корреляции (*локальные переменные*), присвоив им какую-либо функцию, а затем обращаться к ним из правил корреляции, как к обычным полям событий, получая в ответ результат срабатывания функции.

Область применения переменных:

- При поиске группирующих или уникальных значений полей в правилах корреляции.
- В селекторах правил корреляции в фильтрах условий, при которых должно срабатывать правило корреляции.
- При обогащении корреляционных событий. В качестве типа источника следует выбирать **Событие**.
- При наполнении активных листов значениями.

К переменным можно обращаться так же, как к полям события, предваряя их название символом $.

Поля расширенной схемы событий могут использоваться в корреляционных правилах, локальных и глобальных переменных.

Локальные переменные в группирующих и уникальных полях

Вы можете использовать локальные переменных в разделах **Группирующие поля** и **Уникальные поля** правил корреляции типа standard. Для использования локальной переменной необходимо перед ее именем указывать символ "$".

Вы можете ознакомиться с примером использования локальных переменных в разделах **Группирующие поля** и **Уникальные поля** в правиле, поставляемом в Kaspersky SIEM Cloud: R403_Обращение на вредоносные ресурсы с хоста с отключенной защитой или устаревшей антивирусной базой.

Локальные переменные в селекторе

Чтобы использовать локальную переменную в селекторе:

1. Добавьте локальную переменную в правило.
2. В окне **Правила корреляции** перейдите на вкладку **Общие** и добавьте созданную локальную переменную в раздел **Группирующие поля**. Перед именем локальной переменной укажите символ "$".
3. В окне **Правила корреляции** перейдите на вкладку **Селекторы**, выберите существующий фильтр или создайте новый и нажмите на кнопку **Добавить условие.**
4. В качестве операнда выберите **поле события**.
5. В качестве значения поля события укажите локальную переменную и укажите символ "$" перед именем переменной.
6. Укажите остальные параметры фильтра.
7. Нажмите **Сохранить**.

Вы можете ознакомиться с примером использования локальных переменных в правиле, поставляемом с Kaspersky SIEM Cloud: R403_Обращение на вредоносные ресурсы с хоста с отключенной защитой или устаревшей антивирусной базой.

Локальные переменные в обогащении событий

Вы можете использовать правила корреляции типа standard и simple для обогащения событий с помощью локальных переменных.

Обогащение текстом и числами

Обогащение событий можно выполнять с помощью текста (строк). Для этого могут быть использованы функции, позволяющие модифицировать строки: to_lower, to_upper, str_join, append, prepend, substring, tr, replace, str_join.

Обогащение событий можно выполнять с помощью чисел. Для этого могут быть использованы функции: сложение (оператор "+"), вычитание (оператор "-"), умножение (оператор "*"), деление (оператор "/"), round, ceil, floor, abs, pow.

Также для работы с данными в локальных переменных могут быть использованы регулярные выражения.

Применение регулярных выражений в правилах корреляции создает большую нагрузку в сравнении с другими операциями. Поэтому при разработке правил корреляции мы рекомендуем ограничить использование регулярных выражений до необходимого минимума и применять другие доступные операции.

Обогащение временных отметок

Обогащение событий можно выполнять с помощью временных отметок (даты и времени). Для этого могут быть использованы функции, позволяющие получать или модифицировать временные метки: now, extract_from_timestamp, parse_timestamp, format_timestamp, truncate_timestamp, time_diff.

Операции с активными списками и таблицами

Вы можете выполнять обогащение событий с помощью локальных переменных и данных, находящихся в активных списках и таблицах.

Для обогащения событий данными из активного списка необходимо воспользоваться функциями active_list, active_list_dyn.

Для обогащения событий данными из таблицы необходимо воспользоваться функциями table_dict, dict.

Вы можете создавать условные операторы при помощи функции conditional в локальных переменных. Таким образом переменная может вернуть одно из значений в зависимости от того, какие данные поступили для обработки.

Использование локальной переменной для обогащения событий

Чтобы использовать локальную переменную для обогащения событий:

1. Добавьте локальную переменную в правило.
2. В окне **Правила корреляции** перейдите на вкладку **Общие** и добавьте созданную локальную переменную в раздел **Группирующие поля**. Перед именем локальной переменной укажите символ "$".
3. В окне **Правила корреляции** перейдите на вкладку **Действия** и в группе параметров **Обогащение** в раскрывающемся списке **Тип источника данных** выберите **событие**.
4. В раскрывающемся списке **Целевое поле** выберите поле события Kaspersky SIEM Cloud, в которое необходимо передать значение локальной переменной.
5. В раскрывающемся списке **Исходное поле** выберите локальную переменную. Перед именем локальной переменной укажите символ "$".
6. Укажите остальные параметры правила.
7. Нажмите **Сохранить**.

Локальные переменные в обогащении активных листов

Вы можете использовать локальные переменные для обогащения активных листов.

Чтобы выполнить обогащение активного списка при помощи локальной переменной:

1. Добавьте локальную переменную в правило.
2. В окне **Правила корреляции** перейдите на вкладку **Общие** и добавьте созданную локальную переменную в раздел **Группирующие поля**. Перед именем локальной переменной укажите символ "$".
3. В окне **Правила корреляции** перейдите на вкладку **Действия** и в группе параметров **Обновление активных листов** добавьте локальную переменную в поле **Ключевые поля**. Перед именем локальной переменной укажите символ "$".
4. В группе параметров **Сопоставление** укажите соответствие между полями события и полями активного списка.
5. Нажмите на кнопку **Сохранить**.

Свойства переменных

Локальные и глобальные переменные

Свойства глобальных и локальных переменных различаются.

Глобальные переменные:

- Глобальные переменные объявляются на уровне коррелятора и действуют только в пределах этого коррелятора.
- К глобальным переменным коррелятора можно обращаться из всех правил корреляции, которые в нем указаны.
- В правилах корреляции типа standard одна и та же глобальная переменная в каждом селекторе может принимать разные значения.
- Невозможно переносить глобальные переменные между разными корреляторами.

Локальные переменные:

- Локальные переменные объявляются на уровне правила корреляции и действуют только в пределах этого правила.
- В правилах корреляции типа standard областью действия локальной переменной является только тот селектор, в котором переменная была объявлена.
- Локальные переменные можно объявлять в любых типах правил корреляции.
- Невозможно переносить локальные переменные между правилами или селекторами.
- Локальная переменная не может быть использована в качестве глобальной переменной.

Переменные в разных типах правил корреляции

- В правилах корреляции типа **operational** на вкладке **Действия** можно указывать все доступные или объявленные в этом правиле переменные.
- В правилах корреляции типа **standard** на вкладке **Действия** можно указывать только переменные, указанные в этих правилах на вкладке **Общие** в поле **Группирующие поля**.
- В правилах корреляции типа **simple** на вкладке **Действия** можно указывать только переменные, указанные в этих правилах на вкладке **Общие** в поле **Наследуемые поля**.

Требования к переменным

Добавляя функцию переменной необходимо сначала указать название функции, а затем в круглых скобках перечислить ее параметры. Исключением являются простейшие математические операции (сложение, вычитание, умножение, деление), при их использовании скобками обозначается приоритет выполнения операций.

Требования к названиям функций:

- Должно быть уникально в рамках коррелятора.
- Должно содержать от 1 до 128 символов в кодировке Unicode.
- Не может начинаться с символа $.
- Должно быть написано в camelCase или CamelCase.

Особенности указания функций переменных:

- Последовательность указания параметров имеет значение.
- Параметры передаются через запятую: `,`.
- Строковые параметры передаются в одинарных кавычках: `'`.
- Наименования полей событий и переменные указываются без кавычек.
- При обращении к переменной как параметру перед ее названием необходимо добавлять символ `$`.
- Ставить пробел между параметрами необязательно.
- Во всех функциях, где в качестве параметров допускается использование переменной, допускается создавать вложенные функции.

Функции переменных

Операции с активными листами и словарями

Функции active_list и active_list_dyn

Получает данные из активного листа и динамически формирует имя поля активного листа и ключа.

Необходимо указать параметры в следующей последовательности:

1. Название активного листа.
2. Выражение, возвращающее название поля активного листа.
3. Одно или несколько выражений, из результатов которых будет составлен ключ.

Пример

```
active_list('Test', to_lower('DeviceHostName'), to_lower(DeviceCustomString2), to_lower(DeviceCustomString1))
```

Результат: будут получены значения поля активного листа.

С помощью этих функций из переменной можно обратиться к активному листу тенанта Shared. Для этого после названия активного листа необходимо добавить суффикс `@Shared` (регистрозависимый).

Пример

```
active_list('exampleActiveList@Shared', 'score', SourceAddress, SourceUserName)
```

Функция table_dict

Получает данные о значении в указанном столбце словаря типа `таблица`.

Необходимо указать параметры в следующей последовательности:

1. Название словаря.
2. Название столбца словаря.
3. Одно или несколько выражений, из результатов которых будет составлен ключ строки словаря.

Пример

```
table_dict('exampleTableDict', 'office', SourceUserName)
```

Результат: будут получены данные из словаря `exampleTableDict` из строки с ключом `SourceUserName` из столбца `office`.

Пример

```
table_dict('exampleTableDict', 'office', SourceAddress, to_lower(SourceUserName))
```

Результат: будут получены данные из словаря `exampleTableDict` из строки с составным ключом из значения поля `SourceAddress` и значения поля `SourceUserName` в нижнем регистре из столбца `office`.

С помощью этой функции из переменной можно обратиться к словарю тенанта Shared. Для этого после названия активного листа необходимо добавить суффикс `@Shared` (регистрозависимый).

Пример

```
table_dict('exampleTableDict@Shared', 'office', SourceUserName)
```

Функция dict

Получает данные о значении в указанном столбце словаря типа `словарь`.

Необходимо указать параметры в следующей последовательности:

1. Название словаря.

2. Одно или несколько выражений, из результатов которых будет составлен ключ строки словаря.

Пример

```
dict('exampleDictionary', SourceAddress)
```

Результат: будут получены данные из словаря `exampleDictionary` из строки с ключом `SourceAddress`.

Пример

```
dict('exampleDictionary', SourceAddress, to_lower(SourceUserName))
```

Результат: будут получены данные из словаря `exampleDictionary` из строки с составным ключом из значения поля `SourceAddress` и значения поля `SourceUserName` в нижнем регистре.

С помощью этой функции из переменной можно обратиться к словарю тенанта Shared. Для этого после названия активного листа необходимо добавить суффикс `@Shared` (регистрозависимый).

Пример

```
dict('exampleDictionary@Shared', SourceAddress)
```

Операции с контекстными таблицами

Функция context_table

Возвращает значение указанного поля из контекстной таблицы.

Необходимо указать параметры в следующей последовательности:

1. Название контекстной таблицы. Название не должно быть пустым.

2. Название поля, значение которого нужно получить.

3. Название ключевого поля, по которому выполняется сравнение.

4. Выражение, возвращающее значение для сравнения со значением ключевого поля из пункта 3.

Функция должна содержать минимум четыре параметра.

Пример

```
context_table('test_table', 'Username', 'IP', DestinationAddress)
```

Результат: будет получено значение указанного поля из строки контекстной таблицы, для которой ключевое поле совпало со значением, переданным в параметре сравнения. Если таблица или совпадения отсутствуют либо поле не найдено, возвращается пустая строка.

С помощью этой функции из переменной можно обратиться к контекстной таблице тенанта Shared. Для этого после названия контекстной таблицы необходимо добавить суффикс `@Shared` (регистрозависимый).

Пример

```
context_table('test_table@Shared', SourceAddress)
```

Функция len

Возвращает длину строки и массива.

Функция возвращает длину массива, если переданный массив соответствует одному из следующих типов:

- массив целых чисел;
- массив чисел с плавающей точкой;
- массив строк;
- массив логических типов.

Если передан массив другого типа, данные массива приводятся к строковому типу, и функция возвращает длину полученной строки.

Пример

```
len(context_table('tbl1', 'list_field1', 'key1', 'key1_val'))
```

Пример

```
len(DeviceCustomString1)
```

Функция distinct_items

Возвращает список уникальных элементов массива.

Функция возвращает список уникальных элементов массива, если переданный массив соответствует одному из следующих типов:

- массив целых чисел;
- массив чисел с плавающей точкой;
- массив строк;
- массив логических типов.

Если передан массив другого типа, данные массива приводятся к строковому типу, и функция возвращает строку, состоящую из уникальных символов исходной строки.

Пример

```
distinct_items(context_table('tbl1', 'list_field1', 'key1', 'key1_val'))
```

Пример

```
distinct_items(DeviceCustomString1)
```

Функция sort_items

Возвращает отсортированный список элементов массива.

Необходимо указать параметры в следующей последовательности:

1. Выражение, возвращающее объект сортировки.
2. Направление сортировки. Возможные значения: `asc`, `desc`. Если параметр не указан, значение по умолчанию – `asc`.

Функция возвращает отсортированный список элементов массива, если переданный массив соответствует одному из следующих типов:

- массив целых чисел;
- массив чисел с плавающей точкой;
- массив строк.

Функция возвращает список элементов массива в исходном порядке, если был передан массив логических типов.

Если передан массив другого типа, данные массива приводятся к строковому типу, и функция возвращает строку отсортированных символов.

Пример

```
sort_items(context_table('tbl1', 'list_field1', 'key1', 'key1_val'), 'asc')
```

Пример

```
sort_items(DeviceCustomString1)
```

Функция item

Возвращает элемент массива с указанным индексом или символ строки с указанным индексом, если передан массив целых чисел, чисел с плавающей точкой, строк или булевых значений.

Необходимо указать параметры в следующей последовательности:

1. Выражение, возвращающее объект индексирования.
2. Выражение, возвращающее индекс элемента или символа.

Функция должна содержать минимум два параметра.

Функция возвращает элемент массива с указанным индексом или символ строки с указанным индексом, если индекс находится в диапазоне массива и переданный массив соответствует следующему типу:

- массив целых чисел;
- массив чисел с плавающей точкой;
- массив строк;
- массив логических типов.

Если передан массив другого типа и индекс находится в диапазоне массива, данные приводятся к строковому типу и функция возвращает символ строки по индексу. Если передан массив другого типа и индекс не находится в диапазоне массива, функция возвращает пустую строку.

Пример

```
sort_items(context_table('tbl1', 'list_field1', 'key1', 'key1_val'), 'asc')
```

Пример

```
sort_items(DeviceCustomString1)
```

Операции со строками

Функция to_lower

Переводит символы в строке в нижний регистр. Поддерживается для стандартных полей и полей расширенной схемы событий типа `строка`.

Строку можно передать строкой, названием поля или переменной.

Пример

```
to_lower(SourceUserName)
```

Пример

```
to_lower('SomeText')
```

Пример

```
to_lower($otherVariable)
```

Функция to_upper

Переводит символы в строке в верхний регистр. Поддерживается для стандартных полей и полей расширенной схемы событий типа `строка`.

Строку можно передать строкой, названием поля или переменной.

Пример

```
to_upper(SourceUserName)
```

Пример

```
to_upper('SomeText')
```

Пример

```
to_upper($otherVariable)
```

Функция append

Добавляет символы в конец строки. Поддерживается для стандартных полей и полей расширенной схемы событий типа `строка`.

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.
2. Добавляемая строка.

Строки можно передать строкой, названием поля или переменной.

Пример

```
append(Message, '123')
```

Результат: в конец строки из поля `Message` будет добавлена строка `123`.

Пример

```
append($otherVariable, 'text')
```

Результат: в конец строки из переменной `otherVariable` будет добавлена строка `text`.

Пример

```
append(Message, $otherVariable)
```

Результат: в конец строки из поля `Message` будет добавлена строка из переменной `otherVariable`.

Функция prepend

Добавляет символы в начало строки. Поддерживается для стандартных полей и полей расширенной схемы событий типа `строка`.

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.
2. Добавляемая строка.

Строки можно передать строкой, названием поля или переменной.

Пример

```
prepend(Message, '123')
```

Результат: в начало строки из поля `Message` будет добавлена строка `123`.

Пример

```
prepend($otherVariable, 'text')
```

Результат: в начало строки из переменной `otherVariable` будет добавлена строка `text`.

Пример

```
prepend(Message, $otherVariable)
```

Результат: в начало строки из поля `Message` будет добавлена строка из переменной `otherVariable`.

Функция substring

Возвращает подстроку из строки. Поддерживается для стандартных полей и полей расширенной схемы событий типа `строка`.

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.
2. Позиция начала подстроки (натуральное число или 0).
3. Позиция конца подстроки (необязательно).

Строки можно передать строкой, названием поля или переменной. Если номер позиции больше, чем длина строки исходных данных, возвращается пустая строка.

Пример

```
substring(Message, 2)
```

Результат: вернется часть строки из поля `Message` (от третьего символа до конца).

Пример

```
substring($otherVariable, 2, 5)
```

Результат: вернется часть строки из переменной `otherVariable` (от третьего до шестого символа).

Пример

```
substring(Message, 0, len(Message) - 1)
```

Результат: вернется вся строка из поля `Message`, кроме последнего символа.

Функция index_of

Возвращает байтовое смещение символа или подстроки в строке, расчет индекса начинается с 0. Если в результате работы функции подстрока не была найдена, функция вернет отрицательное значение.

Если в строке есть символы, не входящие в набор ASCII, то возвращаемое байтовое смещение не будет соответствовать количеству букв до искомой подстроки.

Доступны следующие параметры функции:

- исходные данные – поле события, другая переменная или константа;
- любое выражение из тех, что доступны в локальных переменных.

Для использования функции необходимо указать параметры в следующей последовательности:

1. Символ или подстрока, позиция которой будет найдена.
2. Строка, по которой будет осуществлен поиск.

Пример

```
index_of('@', SourceUserName)
```

Результат: выполняется поиск символа `@` в поле `SourceUserName`. Поле `SourceUserName` содержит строчку `user@example.com`. Результат = 4. Функция возвращает индекс первой позиции искомого символа в строке. Расчет индекса начинается с 0.

Пример

```
index_of('m', SourceUserName)
```

Результат: выполняется поиск символа `m` в поле `SourceUserName`. Поле `SourceUserName` содержит строчку `user@example.com`. Результат = 8. Функция возвращает индекс первой позиции искомого символа в строке. Расчет индекса начинается с 0.

Функция last_index_of

Возвращает последнюю позицию символа или подстроки в строке, расчет индекса начинается с 0. Если в результате работы функции подстрока не была найдена, функция вернет значение `-9223372036854775808`.

Доступны следующие параметры функции:

- исходные данные – поле события, другая переменная или константа;
- любое выражение из тех, что доступны в локальных переменных.

Для использования функции необходимо указать параметры в следующей последовательности:

1. Символ или подстрока, позиция которой будет найдена.
2. Строка, по которой будет осуществлен поиск.

Пример

```
last_index_of('m', SourceUserName)
```

Результат: выполняется поиск символа `m` в поле `SourceUserName`. Поле `SourceUserName` содержит строчку `user@example.com`. Результат = 15. Функция возвращает индекс последней позиции искомого символа в строке. Расчет индекса начинается с 0.

Функция tr

Убирает в начале и в конце строки указанные символы. Поддерживается для стандартных полей и полей расширенной схемы событий типа `строка`.

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.

2. Строка, которую следует удалить из начала и конца исходной строки (необязательно).

Строки можно передать строкой, названием поля или переменной. Если строку на удаление не указать, в начале и в конце исходной строки будут удалены пробелы.

Пример

```
tr(Message)
```

Результат: в начале и в конце строки из поля `Message` будут удалены пробелы.

Пример

```
tr($otherVariable, '_')
```

Результат: если переменной `otherVariable` соответствует значение `_test_`, будет возвращена строка `test`.

Пример

```
tr(Message, '@example.com')
```

Результат: если в поле события `Message` находится строка `user@example.com`, будет возвращена строка `user`.

Функция replace

Заменяет в строке все вхождения последовательности символов **A** на последовательность символов **B**. Поддерживается для стандартных полей и полей расширенной схемы событий типа `строка`.

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.

2. Строка поиска: последовательность символов, подлежащая замене.

3. Строка замены: последовательность символов, на которую необходимо заменить строку поиска.

Строки можно передать выражением.

Пример

```
replace(Name, 'UserA', 'UserB')
```

Результат: возвращается строка из поля события `Name`, в которой все вхождения `UserA` заменены на `UserB`.

Пример

```
replace($otherVariable, ' text ', '_text_')
```

Результат: возвращается строка из переменной `otherVariable`, в которой все вхождения `' text '` заменены на `'_text_'`.

Функция regexp_replace

Заменяет в строке последовательность символов, удовлетворяющих регулярному выражению, на последовательность символов и группы захвата регулярного выражения. Поддерживается для стандартных полей и полей расширенной схемы событий типа `строка`.

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.
2. Строка поиска: регулярное выражение.
3. Строка замены: последовательность символов, на которую необходимо заменить строку поиска, и идентификаторы групп захвата регулярного выражения. Строку можно передать выражением.

Строки можно передать строкой, названием поля или переменной. Допускается использовать неименованные группы захвата.

В регулярных выражениях, используемых в функциях переменных, каждый символ обратной косой черты необходимо дополнительно экранировать. Например, вместо регулярного выражения `^example\\` нужно указывать выражение `^example\\\\`.

Пример

```
regexp_replace(SourceAddress, '([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3})', 'newIP: $1.$2.$3.10')
```

Результат: возвращается строка из поля события `SourceAddress`, в которой перед IP-адресами вставлен текст `newIP`. Также последние цифры адреса заменены на `10`.

Функция regexp_capture

Получает из исходной строки результат, отвечающий условию регулярного выражения. Поддерживается для стандартных полей и полей расширенной схемы событий типа `строка`.

Необходимо указать параметры в следующей последовательности:

1. Исходная строка.
2. Строка поиска: регулярное выражение.

Строки можно передать строкой, названием поля или переменной. Допускается использовать неименованные группы захвата.

В регулярных выражениях, используемых в функциях переменных, каждый символ обратной косой черты необходимо дополнительно экранировать. Например, вместо регулярного выражения `^example\\` нужно указывать выражение `^example\\\\`.

Пример

```
regexp_capture(Message, '(\\\\d{1,3}\\\\.\\\\d{1,3}\\\\.\\\\d{1,3}\\\\.\\\\d{1,3})')
```

Примеры значений

```
Message = 'Access from 192.168.1.1 session 1'
Message = 'Access from 45.45.45.45 translated address 192.168.1.1 session 1'
```

Результат:

`'192.168.1.1'`

`'45.45.45.45'`

Функция template

Возвращает строку, указанную в функции, с заменой переменных на их значения. Функция `template` может быть использована в одном из двух вариантов:

- Один аргумент – в этом случае можно использовать имена полей для подстановки значений в шаблон.
- Несколько аргументов – в этом случае для подстановки значений используется индекс аргумента, начинающийся с нуля.

Пример

```
template('Текст сообщения: {{.Message}}')
```

Пример

```
template('Имя в нижнем регистре: {{index . 0}}. Имя в верхнем регистре: {{index . 1}}', to_lower(Name),
to_upper(Name))
```

Операции с метками времени

Функция now

Получает временную метку в формате `epoch`. Запускается без аргументов.

Пример

```
now()
```

Функция extract_from_timestamp

Получает атомарные представления времени (в виде год, месяц, день, час, минута, секунда, день недели) из полей и переменных с временем в формате `epoch`.

Параметры необходимо указать в следующей последовательности:

1. Поле события, имеющего тип `timestamp`, или переменная.
2. Обозначение атомарного представления времени. Параметр регистрозависимый.

   Возможные варианты обозначения атомарного времени:

   - y – год в виде числа.
   - M – месяц, числовое обозначение.
   - d – число месяца.
   - wd – день недели: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday.
   - h – часы в 24-часовом формате.
   - m – минуты.
   - s – секунды.
3. Обозначение часового пояса (необязательно).

   Параметр может быть задан в виде строки (например, `Europe/Moscow`) или переменной (`$timezone`). Переменная должна быть предварительно объявлена в локальных переменных правила корреляции. Значение переменной должно содержать строковый идентификатор часового пояса. Также допускается использование переменных, сформированных на основе других переменных и значений словарей.

   Если параметр не указан, время высчитывается в формате UTC.

Пример

```
extract_from_timestamp(Timestamp, 'wd')
```

Пример

```
extract_from_timestamp(Timestamp, 'h')
```

Пример

```
extract_from_timestamp($otherVariable, 'h')
```

Пример

```
extract_from_timestamp(Timestamp, 'h', 'Europe/Moscow')
```

Пример

```
extract_from_timestamp(Timestamp, 'h', $timezone)
```

Пример использования переменной из словаря

```
$key_timezone = 'timezone'
$timezone = dict('UEBA.Timezone', $key_timezone)
```

```
extract_from_timestamp(EndTime, 'h', $timezone)
```

В этом примере переменная `$timezone` формируется на основе другой переменной и значения словаря и используется в качестве параметра `timezone`.

Функция parse_timestamp

Представляет время из формата RFC3339 (например, `2022-05-24 00:00:00`, `2022-05-24 00:00:00+0300`) в формат `epoch`.

Пример

```
parse_timestamp(Message)
```

Пример

```
parse_timestamp($otherVariable)
```

Функция format_timestamp

Представляет время из формата `epoch` в формат RFC3339.

Параметры необходимо указать в следующей последовательности:

1. Поле события, имеющего тип `timestamp`, или переменная.
2. Обозначение формата времени: RFC3339.
3. Обозначение часового пояса (необязательно). Если параметр не указан, время высчитывается в формате UTC.

Пример

```
format_timestamp(Timestamp, 'RFC3339')
```

Пример

```
format_timestamp($otherVariable, 'RFC3339')
```

Пример

```
format_timestamp(Timestamp, 'RFC3339', 'Europe/Moscow')
```

Функция truncate_timestamp

Округляет время в формате `epoch`. После округления время возвращается в формате `epoch`. Время округляется в меньшую сторону.

Параметры необходимо указать в следующей последовательности:

1. Поле события, имеющего тип `timestamp`, или переменная.
2. Параметр округления:
   - 1s – округление до секунд.
   - 1m – округление до минут.
   - 1h – округление до часов.
   - 24h – округление до суток.
3. Обозначение часового пояса (необязательно). Если параметр не указан, время высчитывается в формате UTC.

Пример

```
truncate_timestamp(Timestamp, '1m')
```

Пример округляемого значения: 1654631774175 (7 June 2022 г., 19:56:14.175).

Результат: 1654631760000 (7 June 2022 г., 19:56:00).

Пример

```
truncate_timestamp($otherVariable, '1h')
```

Пример округляемого значения: 1654631774175 (7 June 2022 г., 19:56:14.175).

Результат: 1654628400000 (7 June 2022 г., 19:00:00).

Пример

```
truncate_timestamp(Timestamp, '24h', 'Europe/Moscow')
```

Пример округляемого значения: 1654631774175 (7 June 2022 г., 19:56:14.175).

Результат: 1654560000000 (7 June 2022 г., 0:00:00).

Функция time_diff

Получает интервал времени между двумя метками времени в формате `epoch`.

Параметры необходимо указать в следующей последовательности:

1. Время конца отрезка. Поле события, имеющего тип `timestamp`, или переменная.
2. Время начала отрезка. Поле события, имеющего тип `timestamp`, или переменная.

3. Представление временного интервала:

- ms – в миллисекундах.
- s – в секундах.
- m – в минутах.
- h – в часах.
- d – в днях.

Пример

```
time_diff(EndTime, StartTime, 's')
```

Пример

```
time_diff($otherVariable, Timestamp, 'h')
```

Пример

```
time_diff(Timestamp, DeviceReceiptTime, 'd')
```

Математические операции

Представлены как простейшими математическими операциями, так и функциями.

Простейшие математические операции

Поддерживаются для полей расширенной схемы событий с типом `целое число` и `число с плавающей точкой`.

Операции:

- Сложение.
- Вычитание.
- Умножение.
- Деление.
- Деление по модулю.

Использование круглых скобок определяет последовательность действий.

Доступные аргументы:

- Числовые поля события.
- Числовые переменные.
- Вещественные числа.

При делении по модулю в качестве аргументов можно использовать только натуральные числа.

Ограничения использования:

- Деление на ноль возвращает ноль.
- Математические операции между числами и строками возвращают число в неизменном виде. Например, `1 + abc` вернет `1`.
- Целые числа, полученные в результате операций, возвращаются без точки.

Примеры для `(Type=3; otherVariable=2; Message=text)`	Результат
`Type + 1`	4
`$otherVariable - Type`	-1
`2 * 2.5`	5
`2 / 0`	0
`Type * Message`	0
`(Type + 2) * 2`	10
`Type % $otherVariable`	1

Функция round

Округляет числа. Поддерживается для полей расширенной схемы событий с типом `целое число` и `число с плавающей точкой`.

Доступные аргументы:

- Числовые поля события.
- Числовые переменные.
- Числовые константы.

Примеры для `(DeviceCustomFloatingPoint1=7.75; DeviceCustomFloatingPoint2=7.5 otherVariable=7.2)`	Результат
`round(DeviceCustomFloatingPoint1)`	8
`round(DeviceCustomFloatingPoint2)`	8
`round($otherVariable)`	7

Функция ceil

Округляет числа в большую сторону. Поддерживается для полей расширенной схемы событий с типом `целое число` и `число с плавающей точкой`.

Доступные аргументы:

- Числовые поля события.
- Числовые переменные.
- Числовые константы.

Примеры для `(DeviceCustomFloatingPoint1=7.15; otherVariable=8.2)`	Результат
`ceil(DeviceCustomFloatingPoint1)`	8
`ceil($otherVariable)`	9

Функция floor

Округляет числа в меньшую сторону. Поддерживается для полей расширенной схемы событий с типом `целое число` и `число с плавающей точкой`.

Доступные аргументы:

- Числовые поля события.
- Числовые переменные.
- Числовые константы.

Примеры для `(DeviceCustomFloatingPoint1=7.15; otherVariable=8.2)`	Результат
`floor(DeviceCustomFloatingPoint1)`	7
`floor($otherVariable)`	8

Функция abs

Получает числа по модулю. Поддерживается для полей расширенной схемы событий с типом `целое число` и `число с плавающей точкой`.

Доступные аргументы:

- Числовые поля события.
- Числовые переменные.
- Числовые константы.

Примеры для `(DeviceCustomNumber1=-7; otherVariable=-2)`	Результат
`abs(DeviceCustomFloatingPoint1)`	7
`abs($otherVariable)`	2

Функция pow

Возводит числа в степень. Поддерживается для полей расширенной схемы событий с типом `целое число` и `число с плавающей точкой`.

Параметры необходимо указать в следующей последовательности:

1. База – вещественные числа.
2. Степень – натуральные числа или вещественные числа.

Доступные аргументы:

- Числовые поля события.
- Числовые переменные.
- Числовые константы.

Пример

```
pow(DeviceCustomNumber1, DeviceCustomNumber2)
```

Пример

```
pow($otherVariable, DeviceCustomNumber1)
```

Функция str_join

Объединяет несколько строк в одну с использованием разделителя. Поддерживается для полей расширенной схемы событий с типом `целое число` и `число с плавающей точкой`.

Параметры необходимо указать в следующей последовательности:

1. Разделитель. Строка.
2. Строка 1, строка 2, строка N. Минимум два выражения.

Пример

```
str_join('|', to_lower(Name), to_upper(Name), Name)
```

Результат выполнения команды: строка.

Функция conditional

Получает одно значение в случае выполнения условия и другое значение, если условие не выполнится. Поддерживается для полей расширенной схемы событий с типом `целое число` и `число с плавающей точкой`.

Параметры необходимо указать в следующей последовательности:

1. Условие: строка, синтаксис аналогичен условиям в SQL Where. В условии можно использовать функции переменных Kaspersky SIEM Cloud и ссылаться на другие переменные.
2. Значение при выполнении условия: выражение.
3. Значение при невыполнении условия: выражение.

Поддерживаемые операторы:

- `AND`
- `OR`
- `NOT`
- `=`
- `!=`
- `<`
- `<=`
- `>`
- `>=`
- `LIKE`

  Передается регулярное выражение RE2, а не SQL-выражение.
- `ILIKE`

  Передается регулярное выражение RE2, а не SQL-выражение.
- `BETWEEN`
- `IN`
- `IS NULL`

  Проверка на пустое значение, например 0 или пустую строку.

Пример

```
conditional('SourceUserName = \\'root\\' AND DestinationUserName = SourceUserName', 'match', 'no match')
```

Пример

```
conditional(`DestinationUserName ILIKE 'svc_.*'`, 'match', 'no match')
```

Пример

```
conditional(`DestinationUserName NOT LIKE 'svc_.*'`, 'match', 'no match')
```

Во всех примерах значение зависит от аргументов 2 и 3.

Операции для полей расширенной схемы событий

Для полей расширенной схемы событий типа `строка` поддерживаются следующие функции:

- `len`
- `to_lower`
- `to_upper`
- `append`
- `prepend`
- `substring`
- `tr`
- `replace`
- `regexp_replace`
- `regexp_capture`

Для полей расширенной схемы событий с типом `целое число` или `число с плавающей точкой` поддерживаются следующие простые математические функции:

- `round`
- `ceil`
- `floor`
- `abs`
- `pow`
- `str_join`
- `conditional`

Kaspersky SIEM Cloud поддерживает для полей расширенной схемы событий с типом `массив целых чисел`, `массив чисел с плавающей точкой` и `массив строк` следующие функции:

- Получение i-го элемента массива.

  Пример

  ```
  item(<type>.someStringArray)
  ```

- Получение массива значений.

  Пример

  ```
  <type>.someStringArray
  ```

  Вернется значение `["string1", "string2", "string3"]`.

- Получение количества элементов в массиве.

  Пример

  ```
  len(<type>.someStringArray)
  ```

  Вернется значение `["string1", "string2"]`.

- Получение уникальных записей из массива.

  Пример

  ```
  distinct_items(<type>.someStringArray)
  ```

- Формирование строки с элементами массива в формате TSV.

  Пример

  ```
  to_string(<type>.someStringArray)
  ```

- Сортировка элементов массива.

  Пример

  ```
  sort_items(<type>.someStringArray)
  ```

  В примерах вместо `<type>` необходимо указать тип массива: NA для массива целых чисел, FA для массива чисел с плавающей точкой, SA для массива строк.

Для полей с типом `массив целых чисел` и `массив чисел с плавающей точкой` поддерживаются следующие функции:

- `math_min` – возвращает минимальный элемент массива.

  Пример

  ```
  math_min(NA.NumberArray)
  ```

  Пример

  ```
  math_min(FA.FloatArray)
  ```

- `math_max` – возвращает максимальный элемент массива.

  Пример

  ```
  math_max(NA.NumberArray)
  ```

  Пример

  ```
  math_max(FA.FloatArray)
  ```

- `math_avg` – возвращает среднее значение массива.

  Пример

  ```
  math_avg(NA.NumberArray)
  ```

  Пример

  ```
  math_avg(FA.FloatArray)
  ```

Объявление переменных

Для объявления переменных их необходимо добавить в коррелятор или правило корреляции.

Чтобы добавить глобальную переменную в существующий коррелятор:

1. В веб-интерфейсе в разделе **Мониторинг** → **Ресурсы и сервисы** → **Корреляторы** выберите набор ресурсов нужного коррелятора.

   Откроется мастер установки коррелятора.

2. Выберите шаг мастера установки **Глобальные переменные**.

3. Нажмите на кнопку **Добавить переменную** и укажите следующие параметры:

   - В окне **Переменная** введите название переменной.

     Требования к наименованию переменных

     - Должно быть уникально в рамках коррелятора.
     - Должно содержать от 1 до 128 символов в кодировке Unicode.
     - Не может начинаться с символа $.
     - Должно быть написано в camelCase или CamelCase.

   - В окне **Значение** введите функцию переменной.

     При вводе функций поддерживается автодополнение в виде списка подсказок с возможными вариантами имен функций, их кратким описанием и примерами использования. Вы можете выбрать нужную функцию из списка и вставить ее вместе со списком аргументов в поле ввода.

     Для вызова списка всех подсказок в поле ввода используйте комбинацию клавиш **`Ctrl + Space`**. Для выбора нужной функции из списка используйте клавишу **`Enter`**. Для перехода к следующему аргументу в списке аргументов выбранной функции используйте клавишу **`Tab`**.

     Описание функций переменных.

Переменных можно добавить несколько. Добавленные переменные можно изменить или удалить с помощью значка ✕.

4. Выберите шаг мастера установки **Проверка параметров** и нажмите **Сохранить**.

Глобальная переменная добавлена в коррелятор. К ней можно обращаться, как к полю события, указывая перед названием переменной символ $. Переменная будет использоваться при корреляции после перезапуска сервиса коррелятора.

Чтобы добавить локальную переменную в существующее правило корреляции:

1. В веб-интерфейсе Kaspersky SIEM Cloud в разделе **Мониторинг → Ресурсы и сервисы → Правила корреляции** выберите нужное правило корреляции.

   Откроется окно параметров правила корреляции. Параметры правила корреляции можно также открыть из коррелятора, в которое оно было добавлено, перейдя на шаг мастера установки **Корреляция**.

2. Откройте вкладку **Селекторы**.

3. В селекторе откройте вкладку **Локальные переменные**, нажмите на кнопку **Добавить переменную** и укажите следующие параметры:

   - В окне **Переменная** введите название переменной.

     Требования к наименованию переменных

     - Должно быть уникально в рамках коррелятора.
     - Должно содержать от 1 до 128 символов в кодировке Unicode.
     - Не может начинаться с символа $.
     - Должно быть написано в camelCase или CamelCase.

   - В окне **Значение** введите функцию переменной.

     При вводе функций поддерживается автодополнение в виде списка подсказок с возможными вариантами имен функций, их кратким описанием и примерами использования. Вы можете выбрать нужную функцию из списка и вставить ее вместе со списком аргументов в поле ввода.

     Для вызова списка всех подсказок в поле ввода используйте комбинацию клавиш **`Ctrl + Space`**. Для выбора нужной функции из списка используйте клавишу **`Enter`**. Для перехода к следующему аргументу в списке аргументов выбранной функции используйте клавишу **`Tab`**.

     Описание функций переменных.

   Переменных можно добавить несколько. Добавленные переменные можно изменить или удалить с помощью значка ✕.

   Для правил корреляции типа standard повторите этот шаг для каждого селектора, в которым вы хотите объявить переменные.

4. Нажмите **Сохранить**.

Локальная переменная добавлена в правило корреляции. К ней можно обращаться, как к полю события, указывая перед названием переменной символ $. Переменная будет использоваться при корреляции после перезапуска сервиса коррелятора.

Добавленные переменные можно изменить или удалить. Если правило корреляции обращается к необъявленной переменной (например, если ее название было изменено), в качестве результата возвращается пустая строка.

Если вы измените название переменной, вам потребуется вручную изменить название этой переменной во всех правилах корреляции, где вы ее использовали.

Добавление временного списка исключений для корреляционного правила

Для пользователей без прав редактирования корреляционных правил в веб-интерфейсе Kaspersky SIEM Cloud имеется возможность создавать временный список исключений (например, создавать исключения для ложноположительных срабатываний при работе с алертами). Пользователь с правами редактирования корреляционных правил может затем по необходимости добавить исключения в правило и удалить их из временного списка.

Чтобы добавить исключения в корреляционное правило при работе с алертами:

1. Перейдите в раздел **Алерты** и выберите необходимый алерт.
2. Нажмите на кнопку **Найти в событиях**.

   Отображаются события алерта на странице событий.
3. Откройте корреляционное событие.

   Откроется карточка события, в которой напротив каждого поля отобразится кнопка ⌄ (стрелка) для добавления исключения.
4. Нажмите на кнопку ⌄ и выберите **Добавить в исключение**.

   Открывается боковая панель с полями: **Корреляционное правило**, **Исключение**, **Алерт**, **Комментарий**.
5. Нажать на кнопку **Создать**.

Правило исключения добавлено.

Исключение добавится во временный список. Этот список будет доступен всем, у кого есть права на чтение корреляционных правил, в разделе **Мониторинг → Ресурсы и сервисы → Правила корреляции** в панели инструментов списка правил по кнопке **Список исключений**. Если вы хотите посмотреть исключения конкретного правила, откройте карточку правила и перейдите на вкладку **Исключения**.

Список исключений содержит записи со следующими параметрами:

- `Исключение`

  Условие исключения.
- `Корреляционное правило`

  Наименование корреляционного правила.
- `Алерт`

  Наименование алерта, из которого было добавлено исключение.
- `Тенант`

  Тенант, в рамках которого действует правило и исключение соответственно.

- `Условие`

  Формируется автоматически на основании выбранного поля корреляционного события.

- `Дата создания`

  Дата и время добавления исключения.

- `Истекает`

Дата и время, когда исключение будет автоматически удалено из списка.

- `Создано`

  Имя пользователя, который добавил исключение.

- `Комментарий`

После добавления исключения, корреляционное правило будет работать с учетом исключения в течение 7 дней по умолчанию. В разделе **Параметры** → **Другое** → **Общие** вы можете настроить время действия исключений, изменив параметр `corr_rule_exclusion_ttl_hours` в разделе **Свойства ядра**. Вы можете настроить длительность хранения исключений в часах и днях. Минимальное значение – 1 час, максимальное – 365 дней. Этот параметр доступен только для пользователя с ролью Главный администратор.

Чтобы поля из базовых событий переходили в корреляционные события, эти поля необходимо указать в карточке корреляционного правила на вкладке **Общие** в поле **Наследуемые поля**. Если поля базовых событий не будут отображены в корреляционном событии, поля нельзя будет добавить в исключения.

Чтобы удалить исключения из корреляционного правила:

1. Перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Правила корреляции**.
2. В панели инструментов списка правил нажмите на кнопку **Список исключений**.

   Откроется окно со списком исключений.
3. Выбрать нужные исключения и нажать на кнопку **Удалить**.

Исключения будут удалены из корреляционного правила.

Kaspersky SIEM Cloud генерирует аудит события по факту создания или удаления исключений. Вы можете просмотреть изменения параметров события в окне **Информация о событии**.

Предустановленные правила корреляции

В поставку Kaspersky SIEM Cloud включены перечисленные в таблице ниже правила корреляции.

Предустановленные правила корреляции

Название правила корреляции	Описание
[OOTB] KATA alert	Используется для обогащения событий KATA.
[OOTB] Successful Bruteforce	Срабатывает после выявления успешной попытки аутентификации после множества неуспешных попыток аутентификации. Правило работает на основе событий демона sshd.
[OOTB][AD] Account created and deleted within a short period of time	Выявляет факты создания и последующего удаления учетных записей на хостах на базе ОС Microsoft Windows.
[OOTB][AD] An account failed to log on from different hosts	Выявляет множественные неуспешные попытки аутентификации на различных хостах.

[OOTB][AD] Membership of sensitive group was modified	Работает на базе событий ОС Microsoft Windows.
[OOTB][AD] Multiple accounts failed to log on from the same host	Срабатывает после выявления множественных неуспешных попыток аутентификации на одном хосте от имени разных учетных записей.
[OOTB][AD] Successful authentication with the same account on multiple hosts	Выявляет подключения на разные хосты под одной учетной записью. Правило работает на основе событий ОС Microsoft Windows.
[OOTB][AD] The account added and deleted from the group in a short period of time	Выявляет добавление и последующее удаление пользователя из группы. Правило работает на основе событий ОС Microsoft Windows.
[OOTB][Net] Possible port scan	Выявляет подозрения на сканирование порта. Правило работает на основе событий Netflow, Ipfix.

Пакеты правил корреляции

В файлах, доступных для скачивания, описаны правила корреляции, включенные в поставку Kaspersky SIEM Cloud. Приводятся сценарии, покрываемые правилами, условия их использования и необходимые источники событий.

Правила корреляции можно импортировать в Kaspersky SIEM Cloud. См. раздел онлайн-справки *Импорт ресурсов*.

Ресурсы из репозитория импортируются из репозитория на языке, указанном в параметре **Локализация ресурсов KUMA** в разделе параметров Ядра Kaspersky SIEM Cloud.

Импортированные правила корреляции можно добавлять в используемые вашей организацией корреляторы. См. раздел онлайн-справки *Шаг 3. Корреляция*.

Скачать описание правил корреляции KSC Package

Скачать описание правил корреляции KSMG Package

Скачать описание правил корреляции KATA Package

Скачать описание правил корреляции KUMA Package

Скачать описание правил корреляции Network Package

Скачать описание правил корреляции PCIDSS Package

Скачать описание правил корреляции SOC Content for KUMA

Скачать описание правил корреляции UEBA Package

Скачать описание правил корреляции XDR Package

Скачать описание правил корреляции PostgreSQL Package

Описание пакетов правил корреляции

В поставку Kaspersky SIEM Cloud включены пакеты правил корреляции, перечисленные в таблице ниже.

Название пакета	Описание
[OOTB] SOC Content - RU [OOTB] SOC Content - ENG	Пакеты правил корреляции для KUMA версии 2.1 и выше с русской и английской локализацией. Поддержка этого пакета прекращена.
[OOTB] SOC Content - RU for KUMA 3.2 [OOTB] SOC Content - ENG for KUMA 3.2	Пакеты правил корреляции для KUMA версии 3.2 и выше с русской и английской локализацией. Правила содержат информацию о покрытии матрицы MITRE ATT&CK.
[OOTB] KUMA package - RU [OOTB] KUMA package - ENG	Пакет правил корреляции для мониторинга событий KUMA. Правила корреляции позволяют выявить потенциально опасные действия в системе на основе внутренних событий аудита. Пакет доступен для KUMA версии 3.2 и выше с русской и английской локализацией. По событиям аудита решения обнаруживаются аномалии в поведении пользователей, такие как неудачные попытки входа, подключения с нестандартных IP-адресов и попытки подбора пароля. Также отслеживаются попытки изменения в параметрах решения, включая манипуляции с учетными записями и другими параметрами. Такие действия могут указывать на попытку несанкционированного доступа или обхода механизмов безопасности для проведения дальнейших атак в инфраструктуре компании. Также в пакет входят правила для мониторинга работоспособности служб. Для корректной работы правил необходимо проверить параметры аудита, чтобы журналы событий содержали достаточный уровень детализации.
[OOTB] KSC Package - RU [OOTB] KSC Package - ENG	Пакет правил корреляции, направленных на мониторинг событий Kaspersky Security Center. Пакет доступен для KUMA версии 3.2 и выше с русской и английской локализацией. Он позволяет выявить потенциально опасные действия в системе на основе внутренних событий аудита. Для правильной работы правил корреляции необходимо проверить настройки аудита, чтобы журналы событий содержали достаточный уровень детализации. Пакет правил корреляции работает на событиях, которые собираются через базу данных Kaspersky Security Center. Правила содержат информацию о покрытии матрицы MITRE ATT&CK.
[OOTB] KSMG Package - RU [OOTB] KSMG Package - ENG	Пакет правил корреляции, направленных на мониторинг событий Kaspersky Security Mail Gateway. Пакет доступен для KUMA версии 3.2 и выше с русской и английской локализацией. Он позволяет выявить потенциально опасные действия в системе защиты почтового трафика на основе внутренних событий аудита. Для правильной работы правил необходимо проверить настройки аудита, чтобы журналы событий содержали достаточный уровень детализации. Настройки аудита Kaspersky Secure Mail Gateway расположены в разделе **Параметры → Журналы и события → События**. В блоке **События аудита** нужно выбрать **Уровень журналирования событий аудита → Записывать события аудита и измененные параметры**. Примечания: • Пакет правил работает на событиях в формате CEF. • При отправке событий в SIEM-систему понадобится журнал Kaspersky Secure Mail Gateway в формате CEF (local2). Правила содержат информацию о покрытии матрицы MITRE ATT&CK.
[OOTB] KATA package - RU [OOTB] KATA package - ENG	Пакет правил корреляции для мониторинга событий Kaspersky Anti Targeted Attack (KATA) позволяют выявить потенциально опасные действия в системе на основе внутренних событий аудита. Пакет доступен для KUMA версии 3.2 и выше с русской и английской локализацией. По событиям аудита приложения обнаруживаются аномалии в поведении пользователей, такие как неудачные попытки входа, подключения с нестандартных IP-адресов и попытки подбора пароля. Также отслеживаются попытки изменения в параметрах приложения, включая манипуляции с учетными записями и отключение правил обнаружения. Такие действия могут указывать на попытку несанкционированного доступа или обхода механизмов безопасности для проведения дальнейших атак в инфраструктуре компании. Для корректной работы правил необходимо проверить параметры аудита, чтобы журналы событий содержали достаточный уровень детализации.
[OOTB] Network Package - RU [OOTB] Network Package - ENG	Пакет правил корреляции, направленных на выявление аномалий в сетевой активности, для KUMA версии 3.2 и выше с русской и английской локализацией. Правила содержат информацию о покрытии матрицы MITRE ATT&CK. Пакет также содержит панели мониторинга.
[OOTB] PCIDSS Package - RU [OOTB] PCIDSS Package - ENG	Пакет правил корреляции, направленных на соблюдение требований стандарта PCI DSS. Пакет доступен для KUMA версии 3.2 и выше с русской и английской локализацией. Этот пакет также содержит панели мониторинга. Для правильной работы набора ресурсов необходимо добавить поле расширенной схемы событий **S.Compliance_PCIDSS_Requirements** в разделе **Настройки → Другое → Поля расширенной схемы событий**. Правила содержат информацию о покрытии матрицы MITRE ATT&CK.

Название пакета	Описание
[OOTB] XDR package - RU [OOTB] XDR package - ENG	Пакет содержит набор ресурсов для обнаружения продвинутых атак в инфраструктуре. Пакет доступен для KUMA версии 3.2 и выше с русской локализацией. С его помощью можно обнаружить не только попытки использования наиболее популярного, по версии Kaspersky MDR, вектора получения первоначального доступа - фишинга, но и вирусного заражения, попытки обхода средств защиты, доставки и запуска полезной нагрузки, закрепления, разведки, бокового перемещения и связи с сервером управления различными способами. Правила работают на событиях продуктов "Лаборатории Касперского": EDR, KSC, KSMG, а также используют события операционных систем семейства Windows. Правила содержат информацию о покрытии матрицы MITRE ATT&CK.
[OOTB] UEBA package - RU [OOTB] UEBA package - ENG	Beta-версия пакета правил корреляции. Пакет правил корреляции предназначен для выявления аномального поведения учетной записи или рабочей станции в корпоративной сети. Пакет доступен для KUMA версии 3.2 и выше с русской и английской локализацией. Он строит адаптивные модели нормального поведения на основе накопленных исторических данных (сбор данных длится месяц или заданный период). Эти модели используются для расчета статистических показателей, минимизирующих ложные срабатывания и эффективно выявляющих потенциально опасные отклонения. Источники данных: События ОС Windows, NetFlow, Cisco, Solar Proxy. Примечания: • Правила сбора данных (collection rules) могут быть адаптированы под конкретные средства защиты информации и источники телеметрии. • Для максимальной эффективности работы пакета критически важно обогащение событий данными DNS. • Правила могут оказать воздействие на производительность коррелятора. • Рекомендуется использовать правила в KUMA версии 4.0 и выше. Правила содержат информацию о покрытии матрицы MITRE ATT&CK.
[OOTB] NCCCI package - RU for KUMA 4.0	Пакет включает в себя набор панелей мониторинга и шаблонов отчетов, которые визуализируют детализированную информацию о нарушениях, классифицированных по категориям и типам инцидентов безопасности Национального координационного центра по компьютерным инцидентам (НКЦКИ). Визуализация строится на основе значений поля S.Compliance_NCCCI_IncidentClassification, которое автоматически заполняется правилом обогащения для правил из пакета SOC package. Перед импортом пакета визуализации необходимо создать строковое поле расширенной схемы событий S.Compliance_NCCCI_IncidentClassification, либо убедиться в его наличии. Данный пакет также содержит панели мониторинга.
[OOTB] FSTEC package - RU for KUMA 4.0	Пакет включает в себя набор панелей мониторинга и шаблонов отчетов, которые визуализируют детализированную информацию о нарушениях защитных мер, рекомендуемых ФСТЭК России для предотвращения угроз и устранения уязвимостей согласно информации Банка данных угроз безопасности информации. Визуализация строится на основе значений поля S.Compliance_FSTEC_ProtectiveMeasures, которое автоматически заполняется правилом обогащения для правил из пакета SOC package. Перед импортом пакета визуализации необходимо создать строковое поле расширенной схемы событий S.Compliance_FSTEC_ProtectiveMeasures, либо убедиться в его наличии. Данный пакет также содержит панели мониторинга.
[OOTB] PostgreSQL package - RU [OOTB] PostgreSQL package - ENG	Пакет правил корреляции для мониторинга событий PostgreSQL. Правила корреляции позволяют выявлять потенциально опасные действия в системе на основе внутренних событий аудита. По событиям аудита приложения обнаруживаются аномалии в поведении пользователей, такие как сбор информации об учетных записях, попытки выполнения произвольного кода в системе, а также запись и чтение данных из файловой системы. Для корректной работы правил корреляции необходимо проверить настройки аудита, чтобы журналы событий содержали достаточный уровень детализации.

Автоматическое подавление срабатывания правил

В пакете с правилами корреляции SOC_package предусмотрено автоматическое подавление срабатывания правил, если частота срабатывания превышает пороговые значения.

Опция автоматического подавления предполагает следующую логику работы: если правило сработало более 100 раз за 1 минуту и такое поведение случилось не менее 5 раз за 10 минут, правило будет помещено в стоп-лист.

- При первом помещении в стоп-лист правило отключается на 1 час.
- При повторном - на 24 часа.
- При всех последующих на 7 дней.

Логика работы описана в ресурсах: правилах, активных листах и словарях, которые размещены в папке SOC_package/System/Rule disabling by condition.

Вы можете задать параметры и пороговые значения с учетом своих потребностей.

Чтобы включить опцию автоматического подавления, в словаре SOC_package/Integration/Rule disabling configuration присвойте параметру **enable** значение `1`.

Чтобы отключить опцию автоматического подавления, в словаре SOC_package/Integration/Rule disabling configuration присвойте параметру **enable** значение `0`.

По умолчанию автоматическое подавление включено и параметру **enable** присвоено значение `1`.

События аудита

В правилах корреляции из набора ресурсов [OOTB] SOC Content используются события аудита, перечисленные в таблице ниже.

События аудита

Источник событий	События аудита
CheckPoint	Anti Malware, Threat Emulation
Cisco ASA, FTD, PIX	106021, 320001, 322001, 322002, 322003, 405001, 405002
CyberTrace	alert
DNS	query
KATA	TAA has tripped on events database
KSC	GNRL_EV_ATTACK_DETECTED, GNRL_EV_SUSPICIOUS_OBJECT_FOUND, GNRL_EV_VIRUS_FOUND, GNRL_EV_WEB_URL_BLOCKED, KLSRV_HOST_STATUS_CRITICAL, KLSRV_HOST_STATUS_OK, KLSRV_HOST_STATUS_WARNING
KSMG	LMS_EV_SCAN_LOGIC_AV_STATUS, LMS_EV_SCAN_LOGIC_KT_STATUS, LMS_EV_SCAN_LOGIC_CF_STATUS, LMS_EV_SCAN_LOGIC_AP_STATUS
KUMA	Correlation rule
Windows Event Log Powershell	4103, 4104
Windows Event Log Security	1102, 4624, 4625, 4656, 4657, 4662, 4663, 4672, 4688, 4697, 4720, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4738, 4768, 4769, 4771, 5136, 5140, 5145
Windows Event Log System	7036, 7045
Windows Event Log Defender	1006, 1015, 1116, 1117, 5001, 5010, 5012, 5101
Netflow, FW	Traffic log
Palo Alto	virus
auditd	ADD_USER, DEL_USER, PATH, SYSCALL, USER_AUTH, USER_LOGIN, execve

Корреляция с использованием активов и категорий активов

Kaspersky SIEM Cloud позволяет использовать категории активов в правилах корреляции. Такие правила корреляции более универсальные, так как охватывают большее количество активов, чем правила корреляции, направленные на конкретные активы. Например, вы можете настроить срабатывание правила корреляции, если в качестве источника обнаружен актив из одной категории, а в качестве назначения – из другой.

Настройка правил корреляции с использованием категорий активов состоит из следующих этапов:

❶ Добавление активов в Kaspersky SIEM Cloud

Активы добавляются в Kaspersky SIEM Cloud либо вручную, либо через импорт из других решений, например из Kaspersky Security Center. Всем добавленным активам Kaspersky SIEM Cloud присваивает идентификатор актива `AssetID`. При поступлении события в Kaspersky SIEM Cloud в полях этого события нет значения `AssetID`, то есть нет информации о том, какие именно активы из списка добавленных в Kaspersky SIEM Cloud были затронуты. Обогащение событий информацией об активах происходит в коллекторе.

❷ Настройка обогащения событий информацией об активах на коллекторах

Так как обогащение активами повышает нагрузку на сервис коллектора, рекомендуется выбрать, на каких коллекторах вы хотите настроить обогащение активами. Это можно сделать исходя из типа и функции источников событий, которые отправляют события в коллектор. Вы можете настроить обогащение активами на всех коллекторах и позднее выключить обогащение на тех коллекторах, для которых оно не требуется.

Обогащение событий активами вы можете настроить на шаге **Обогащение событий** при создании коллектора. Для этого вам нужно создать и настроить правило обогащения с типом **обогащение активами**. Вы можете это сделать либо на шаге **Обогащение событий**, либо создать правило обогащения предварительно и затем привязать его в коллекторе.

Логика работы правила обогащения активами следующая. Когда в коллектор поступает событие, Kaspersky SIEM Cloud проверяет, заполнены ли поля `SourceAddress`, `DestinationAddress`, `DeviceAddress`, `SourceHostName`, `DestinationHostName` и `DeviceHostName`. Значения IP-адреса или FQDN из этих полей затем сверяются со значениями IP-адресов и FQDN из свойств активов, добавленных в Kaspersky SIEM Cloud. Таким образом, совпадение значений из полей события и из свойств актива позволяет определить, какой именно актив указан в событии. Далее Kaspersky SIEM Cloud прописывает значение `AssetID` найденного актива в одно или несколько из следующих полей события: `SourceAssetID`, `DestinationAssetID`, `DeviceAssetID`. После этого события направляются в коррелятор или хранилище.

❸ Добавление категорий активов

Вы можете создать категории активов, чтобы объединить их в логические группы на основе какого-либо признака.

❹ Настройка корреляции с использованием категорий активов

Коррелятор получает нормализованное событие. Если в этом событии прописаны значения `AssetID`, коррелятор через запрос к базе данных Ядра Kaspersky SIEM Cloud получает информацию о принадлежности этого актива категориям активов. Таким образом, на основе этой информации вы можете создавать правила корреляции, в которых в качестве условий срабатывания можно указать категории активов.

Например, для обнаружения атаки "Попытка доступа непривилегированного пользователя к критическим элементам инфраструктуры" вы можете создать правило корреляции и указать на вкладке **Селекторы** фильтр:

```
SourceAssetID inCategory "Устройства непривилегированных пользователей"
И
DestinationAssetID inCategory "Оборудование инфраструктуры"
И
DestinationPort = ИЛИ (22, 3389, 1433)
```

При таких параметрах при поступлении события о попытке доступа с устройства из категории "Устройства непривилегированных пользователей" на устройство из категории "Оборудование инфраструктуры" по порту 22, 3389 или 1433 Kaspersky SIEM Cloud выполнит следующие действия:

1. На коллекторе будут определены активы, которые соответствуют IP-адресам устройства-источника и устройства-назначения.

   a. Коррелятор последовательно выполнит следующее:

   b. Определит, в какие категории входят эти активы.

   c. Применит фильтр, указанный в правиле корреляции.

   d. При выполнении условий фильтра создаст корреляционное событие.

2. В веб-интерфейсе будет создан алерт.

5 Реагирование

Вы можете запускать задачи на конкретных активах вручную в окне информации об активе или автоматически с помощью правил реагирования.

Техники и тактики MITRE ATT&CK

Все операции с техниками и тактиками MITRE ATT&CK доступны только после импорта списка техник MITRE ATT&CK.

В Kaspersky SIEM Cloud доступны следующие возможности:

- Обогащение корреляционных событий информацией о техниках и тактиках MITRE ATT&CK.

  Для этого используются поля модели данных события Tactic и Technique. При генерации корреляционного события можно заполнять эти поля соответствующими данными для последующего использования. Например, при получении нового алерта с разметкой по MITRE ATT&CK, вы можете открыть сайт MITRE ATT&CK и ознакомиться с описанием техник и тактик, когда, каким образом и для чего злоумышленники могут использовать эти техники, как их обнаруживать и митигировать риски - все это поможет разработать план реагирования. Также вы можете строить отчеты и панели мониторинга, исходя из того, какие алерты и техники были замечены в инфраструктуре. Если вы используете правила корреляции из пакета SOC_package и хотите настроить обогащение корреляционных событий информацией о техниках и тактиках MITRE ATT&CK, добавьте в корреляторе правила обогащения MITRE.

- Оценка покрытия матрицы MITRE ATT&CK вашими корреляционными правилами.

  В этом случае используются общие настройки корреляционного правила, где есть возможность привязать к каждому правилу соответствующие техники MITRE. Этот параметр используется для описания самого правила и эти данные никак не передаются в корреляционное правило или алерт. Привязка техник и тактик к правилам корреляции позволяет проанализировать покрытие матрицы MITRE ATT&CK, фокусируясь на техниках, наиболее релевантных для конкретной инфраструктуры.

Если вы хотите оценить покрытие матрицы MITRE ATT&CK вашими корреляционными правилами, выполните следующие шаги:

1. Скачайте справочник техник из официального репозитория MITRE ATT&CK и импортируйте справочник техник в Kaspersky SIEM Cloud.
2. Привяжите техники MITRE ATT&CK к правилам корреляции.
3. Экспортируйте правила корреляции в MITRE ATT&CK Navigator.

В результате вы сможете визуально оценить покрытие матрицы MITRE ATT&CK.

- Визуализация покрытия матрицы MITRE ATT&CK продуктами "Лаборатории Касперского".

Импорт списка техник MITRE ATT&CK

Импорт списка техник MITRE ATT&CK доступен только пользователю с ролью Главный администратор.

Чтобы импортировать список техник MITRE ATT&CK:

1. Скачайте справочник техник MITRE ATT&CK на портале GitHub.

   Kaspersky SIEM Cloud поддерживает работу только со справочником техник MITRE ATT&CK начиная с версии 14.2, рекомендуемая версии справочника для использования 19.2.

2. В веб-консоли перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Общее**.
3. В разделе **Настройки списка техник MITRE** нажмите на кнопку **Импортировать из файла**.

   Откроется окно выбора файлов.

4. Выберите скачанный справочник техник MITRE ATT&CK и нажмите на кнопку **Открыть**.

   Окно выбора файлов закроется.

Список техник MITRE ATT&CK будет импортирован в Kaspersky SIEM Cloud. Вы можете увидеть список импортированных техник и версию справочника техник MITRE ATT&CK, нажав на кнопку **Просмотреть список**.

Добавление в коррелляторе правил обогащения MITRE

Правила обогащения **MITRE Technique** и **MITRE Tactics** предназначены и применяются для обогащения только правил корреляции, импортированных из пакета SOC_package. Если в коррелляторе используются пользовательские правила корреляции, добавление правил обогащения **MITRE Technique** и **MITRE Tactics** не приводит к их автоматическому обогащению.

Чтобы добавить правила обогащения MITRE:

1. Убедитесь, что выполнен импорт списка техник MITRE.
2. В веб-консоли перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Коррелляторы** нажмите **Создать**, чтобы создать коррелятор, или выберите действующий коррелятор в списке, чтобы перейти в режим редактирования параметров.
3. В разделе **Обогащение** нажмите **Добавить обогащение**.
4. В открывшемся окне в раскрывающемся списке **Правило обогащения** выберите правила **MITRE Technique** и **MITRE Tactics**.

5. Сохраните параметры коррелятора.

6. Если вы создали коррелятор, необходимо выполнить установку сервиса коррелятора на хосте. Если вы редактировали параметры действующего коррелятора, сервис коррелятора необходимо перезапустить.

Правила обогащения **MITRE Technique** и **MITRE Tactics** добавлены.

Привязка техник MITRE ATT&CK к правилам корреляции

Чтобы привязать техники MITRE ATT&CK к правилам корреляции:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Правила корреляции**.

2. Откройте окно редактирования правила корреляции, нажав на имя правила корреляции.

   Откроется окно редактирования правила корреляции.

3. Во вкладке **Общие** при нажатии на поле **Техники MITRE** откроется список доступных техник. Для удобства поиска доступен фильтр: в поле можно ввести название техники, ID техники или тактики. Для привязки к правилу корреляции доступна одна или несколько техник MITRE ATT&CK.

4. Нажмите на кнопку **Сохранить**.

Техники MITRE ATT&CK будут привязаны к правилу корреляции. В веб-интерфейсе в разделе **Мониторинг → Ресурсы и сервисы → Правила корреляции** в столбце **Техники MITRE** у отредактированного правила отобразится ID выбранной техники, а при наведении курсора на элемент отобразится полное название техники с указанием ID техники и тактики.

Экспорт правил корреляции в MITRE ATT&CK Navigator

Чтобы экспортировать правила корреляции с привязанными техниками в MITRE ATT&CK Navigator:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Правила корреляции**.

2. В правом верхнем углу нажмите на кнопку **...**.

3. В раскрывающемся списке нажмите на кнопку **Экспортировать в MITRE ATT&CK Navigator**.

4. В открывшемся окне выберите правила корреляции, которые вы хотите экспортировать.

5. Нажмите на кнопку **OK**.

   Файл с экспортированными правилами будет загружен на ваш компьютер.

6. Загрузите файл с вашего компьютера в MITRE ATT&CK Navigator для оценки покрытия матрицы MITRE ATT&CK.

Вы можете произвести проверку покрытия матрицы MITRE ATT&CK.

Конвертер правил Sigma

Конвертер правил Sigma преобразует правила корреляции в формат, поддерживаемый Kaspersky SIEM Cloud, и упрощает импорт простых правил для последующей доработки аналитиком.

Список операционных систем, на которых поддерживается работа конвертера правил Sigma, приведен в разделе Программные требования.

Чтобы использовать конвертер правил Sigma для преобразования правил корреляции:

1. Установите конвертер правил Sigma. Доступны следующие варианты установки:

   Установка конвертера правил Sigma с использованием docker и bash

   Этот метод установки подходит для локальной установки веб-интерфейса конвертера.

   Для установки требуются последние версии bash и docker. Для подробной информации по развертыванию bash и docker обратитесь к официальной документации.

   Astra Linux 1.7 не поддерживается.

   Чтобы установить конвертер:

   1. Войдите в директорию с распакованным архивом и выполните одну из команд:

      - Чтобы установить конвертер на хост с адресом `0.0.0.0:8000`, выполните следующую команду:

        ```
        ./run.sh
        ```

      - Чтобы установить конвертер на хост с адресом `0.0.0.0` и другим портом, например `8888`, выполните следующую команду:

        ```
        ./run.sh <port>
        ```

        где:

        `<port>` – порт (порт по умолчанию `8000`).

      - Чтобы установить конвертер на хост с адресом `127.0.0.1:9999`, выполните следующую команду:

        ```
        ./run.sh <IP address>:<port>
        ```

        где:

        - `<IP address>` – IP-адрес слушающего интерфейса, по умолчанию `0.0.0.0`. Указывайте `127.0.0.1` для запуска только на локальном интерфейсе.
        - `<port>` – порт.

   Конвертер будет установлен.

   Установка конвертера правил Sigma в среде, допускающей запуск образов docker

Этот метод установки использует предоставленный контейнер и позволяет создать сервис systemd и развернуть веб-интерфейс с помощью Kubernetes.

Подойдет любой инструмент запуска контейнеров, например docker, podman или cri-o. Установка заключается в загрузке образа контейнера и последующего запуска образа с указанием нужного порта.

Чтобы установить конвертер с помощью podman:

1. Загрузите образ контейнера:

```
podman load --input "kuma-sigma-converter-x.x.x.tar
```

2. Запустите образ одним из следующих способов:

   - С помощью команды:

     ```
     podman run --name=kuma-converter -p "8000:8000" -e "PORT=8000" --rm -it kuma-sigma-converter:x.x.x
     ```

     Дождитесь, когда команда будет выполнена или перейдет в состояние ожидания. Не нажимайте **Ctrl**+**C**, пока процесс установки не будет завершен или пока не будет явно предложено прервать установку

   - Запуск в фоновом режиме:

     ```
     podman run --name=kuma-converter -p "8000:8000" -e "PORT=8000" --rm kuma-sigma-converter:x.x.x
     ```

Конвертер будет установлен.

Установка конвертера правил Sigma с использованием Python 3.10 и выше

Этот метод установки отличается наибольшей гибкостью и подходит опытным пользователям, поскольку вы можете адаптировать конвертер под свои потребности. В отличие от других методов, этот метод требует подключения к интернету для скачивания пакетов Python.

Чтобы установить конвертер:

1. Убедитесь, что установлен Python 3.10 или выше.

2. Установите poetry для управления зависимостями Python. Для Ubuntu или Debian можно воспользоваться менеджером пакетов:

   ```
   sudo apt-get update
   sudo apt install pipx
   pipx install poetry
   ```

3. Используйте poetry для настройки и запуска веб-интерфейса конвертера правил Sigma:

   ```
   cd sigconverter.io
   poetry install
   poetry run ./run.py
   ```

4. В браузере перейдите на хост, где установлен веб-интерфейс конвертера правил Sigma. Для локальной установки адрес будет следующим: `http://127.0.0.1:8000` или `http://0.0.0.0:8000`.

5. При необходимости укажите переменные окружения `HOST` и `PORT`, чтобы настроить слушающий интерфейс и задать номер порта.

Конвертер будет установлен.

Поскольку конвертер правил Sigma представляет собой плагин для инфраструктуры pySigma, допускается использование pySigma-backend-kuma с другими стандартными инструментами Sigma, не только настраиваемой версией sigconverter.io. Например:

- sigma-cli – конвертер с интерфейсом командной строки.
- sigconverter.io – исходный универсальный веб-интерфейс.

Файлы README для библиотек, представленных в исходном коде:

- `src/pySigma/README.md` – инфраструктура и библиотека промышленного стандарта преобразования sigma.
- `src/pySigma-backend-kuma/README.md` – плагин для pySigma, который реализует преобразование фильтров и запросов Kaspersky SIEM Cloud.
- `src/sigconverter.io/README.md` – пользовательский веб-интерфейс.

После установки войдите в веб-интерфейс конвертера.

2. Адаптируйте правило корреляции в конвертере правил Sigma и скопируйте или импортируйте адаптированное правило в Kaspersky SIEM Cloud.

3. Перезапустите коррелятор, чтобы применить изменения.

Адаптированное вами правило корреляции будет применяться в корреляторе.

Подготовка правила Sigma

Чтобы конвертировать правило Sigma в правило Kaspersky SIEM Cloud:

1. Перед адаптацией правила убедитесь, что соблюдены следующие требования:

   - Поскольку в предустановленных нормализаторах используется обогащение событий `to lower case` для полей, содержащих имена пользователей, имена хостов, имена процессов, мы рекомендуем в исходном правиле Sigma приводить соответствующие поля к нижнему регистру.
   - Мы не рекомендуем добавлять комментарии или дополнительную информацию в условия contains и другие условия проверки содержимого строк. Если нужно добавить комментарий, используйте символ #. Комментарий не повлияет на условие.
   - Правило должно начинаться со слова `title`, дефисов перед ним не должно быть.

2. Скопируйте из веб-интерфейса Kaspersky SIEM Cloud правило корреляции, которое вы хотите изменить, конвертируйте его в формат YML и вставьте на вкладку конвертера **rule.yml**. Выберите в раскрывающихся списках нужные параметры. Если при проверке обнаружены ошибки, исправьте их.

3. В конвертере правил Sigma в поле **Backend** выберите **kuma**, в поле **Format** выберите **default**, поле **Pipeline** оставьте пустым.

   Доступны следующие значения:

   - Backend: kuma, Format: default – готовый для запуска SQL-запрос без форматирования.
   - Backend: kuma, format: SQL_formatted – готовый для запуска SQL-запрос с форматированием.
   - Backend: kuma_filter, Format: default – готовый селектор для правила корреляции.
   - Backend: kuma_filter, Format: correlation – готовое для импорта правило корреляции в формате JSON. Для импорта вы можете использовать метод REST API /api/v3/resources/correlationRule/create с указанием tenantID и названия тенанта для импорта.

4. Перейдите на вкладку конвертера **custom_pipeline.yml** и скопируйте на эту вкладку пример словаря, адаптированный под pySigma.

   Пример словаря, адаптированный под pySigma

   Windows process_creation mapping

   product: windows

   category: process_creation

   DeviceEventClassID = 4688

   Windows sysmon EVENT=11 mapping

   product: windows

   service: Sysmon

   EventID = 11

   Windows security

   product: windows

   service: security

   EventID = 4624|4662|4104|4698

```
name: KUMA windows
priority: 30
transformations:
### Windows process_creation mapping

  - id: MAPPING_logsource_windows_process_creation
    type: field_name_mapping
    mapping:
      ParentImage: SourceProcessName
      Image: DestinationProcessName
      CommandLine: DeviceCustomString4
    rule_conditions:
```

```
      - type: logsource
        product: windows
        category: process_creation

  - id: DEFAULT_FOR_logsource_windows_process_creation
    type: add_condition
    conditions:
      DeviceVendor: Microsoft
      DeviceProduct: Windows
      DeviceEventClassID: '4688'
    rule_conditions:
       - type: logsource
         product: windows
         category: process_creation

### Windows sysmon EventID=11 mapping
  - id: DEFAULT_FOR_logsource_windows_sysmon
    type: add_condition
    conditions:
      DeviceVendor: Microsoft
      DeviceProduct: Sysmon
    rule_conditions:
       - type: logsource
         product: windows
         service: Sysmon

  - id: MAPPING_logsource_windows_sysmon
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      Image: OldFilePath
      CommandLine: DeviceCustomString4
      TargetFilename: FilePath
    rule_conditions:
      - type: logsource
        product: windows
        service: Sysmon

### Windows security mapping
  - id: DEFAULT_FOR_logsource_windows_security
    type: add_condition
    conditions:
      DeviceVendor: Microsoft
      DeviceProduct: Windows
    rule_conditions:
       - type: logsource
         product: windows
         service: security

  - id: DEFAULT_MAPPING_FOR_logsource_windows_security
    type: field_name_mapping
    mapping:
      Computer: DestinationHostName
      LogonID: FlexString1
    rule_conditions:
       - type: logsource
         product: windows
         service: security

  - id: 4624_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      LogonType: DeviceCustomNumber1
      SourceIP: SourceAddress
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: 4624

  - id: 4662_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      Properties: FilePermission
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: 4662

  - id: 4104_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
```

```
    mapping:
      EventID: DeviceEventClassID
      ScriptBlockText: Message
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: 4104

  - id: 4698_CONDITIONAL_MAPPING_logsource_windows_security
    type: field_name_mapping
    mapping:
      EventID: DeviceEventClassID
      TaskName: SourceProcessName
    rule_conditions:
      - type: contains_detection_item
        field: "EventID"
        value: '4698'
```

На вкладке **query** отобразится результат конвертации правила. В зависимости от сценария полученный результат можно использовать следующим образом:

- использовать как SQL-оператор в запросе Kaspersky SIEM Cloud;
- использовать как фильтр в корреляционном правиле Kaspersky SIEM Cloud;
- импортировать в Kaspersky SIEM Cloud в формате JSON как корреляционное правило по одному правилу.

Поддерживаемые примеры конвертации правил Sigma

Правило Sigma	Сопоставление с объектами Kaspersky SIEM Cloud	
title: Generic-DCSync Execution id: 9107f781-c984-436a-8093-1aaa64c70c49 description: Detects access to DC with "DS-Replication-Get-Changes" or "DS-Replication-Get-Changes-All" rights author: Kaspersky status: stable modified: 2023-08-02 tags: - attack.credential_access - attack.t1003.006 logsource: product: windows service: security detection: selection1: EventID: 4662 Properties|contains: - 'DS-Replication-Get-Changes' - '1131f6aa-9c07-11d1-f79f-00c04fc2dcd2' - '1131f6ad-9c07-11d1-f79f-00c04fc2dcd2' selection2: EventID: 4624 LogonType: 3 filter: EventID: 4624 LogonType: 3 SourceIP: - '<ip address of DC servers>' timeframe: 1m condition: selection1 or (selection2 and not filter) | count(EventID) by Computer,LogonID = 2 fields: - SourceIP - Computer - LogonID - Username - Properties falsepositives: - Unknown level: high	Нормализатор "Microsoft products" tags → description logsource DeviceVendor = Microsoft DeviceProduct = Windows selection1: DeviceEventClassID=4662 FilePermission contains '' OR FilePermission contains '' OR FilePermission contains '' selection2 DeviceEventClassID=4624 DeviceCustomNumber1 = 3 filter DeviceEventClassID=4624 DeviceCustomNumber1 = 3 SourceAddress = <IP> condition: DeviceVendor = Microsoft AND DeviceProduct = Windows AND ((DeviceEventClassID=4662 FilePermission contains '' OR FilePermission contains '' OR FilePermission contains '') OR ((DeviceEventClassID=4624 AND DeviceCustomNumber1 = 3) NOT (DeviceEventClassID=4624 AND DeviceCustomNumber1 = 3 AND SourceAddress = <IP>))) все, что внутри Count() EventID передать в Unique fields, все, что после 'by' Computer → DestinationHostName LogonID → FlexString1 передать в Aggregation fields, все, что после '=' или '>' 2 передать в threshold. timeframe передать в time window	Для корреляцион реализована част условия condition условие селектор запрос для Поиск

Правило Sigma	Сопоставление с объектами Kaspersky SIEM Cloud	
title: Lsass Dump via LOLBin id: 2fe9cd33-d7f1-4d52-ab11-e40cb359ad02 description: detects lsass dump via lolbins such as procdump.exe, dotnet-dump.exe, dumpminitool.exe references: - https://twitter.com/bohops/status/1635288066909966338 - https://twitter.com/mrd0x/status/1511415432888131586 modified: 2023-07-18 author: Kaspersky status: stable tags: - attack.credential_access - attack.t1003.001 logsource: product: windows category: process_creation detection: selection_procdump: Image|endswith: - '\procdump.exe' - '\procdump64.exe' CommandLine|contains: 'lsass' selection_dotnet: Image|endswith: '\dotnet-dump.exe' CommandLine: ' collect ' selection_dumpminitool: Image|endswith: '\dumpminitool.exe' condition: 1 of selection* falsepositives: - Unknown level: high	Конвертируется так же, как и правило в строке 3 таблицы. Отличие: в условии `condition` используется конструкция `1 of selection`, где `selection` обозначает одну из именованных групп условий.	DeviceVendor=' DeviceProduct= DeviceEventCla (((Desti '\\procdump.ex '\\procdump64. 'lsass') OR (Destinati dump.exe' AND De) OR Destinati '\\dumpminitoo)
title: Generic-Clearing Windows Event Logs via Command Line id: a903492e-da40-4ab4-a92d-306a4799d973 description: Detects Clear Windows Event Logs via Command Line author: Kaspersky status: stable modified: 2023-07-18 tags: - attack.defense_evasion - attack.t1070.001 logsource: product: windows category: process_creation detection: selection1: Image|endswith: '\wevtutil.exe' CommandLine|contains: - ' cl ' - 'clear' selection2: Image|endswith: - '\powershell.exe' - '\powershell_ise.exe' - '\pwsh.exe' CommandLine|contains: - 'Clear-EventLog' - 'Remove-EventLog' selection3: Image|endswith: '\wmic.exe' CommandLine|contains: - 'ClearEventLog' condition: 1 of them falsepositives: - Legitimate System Administrator actions level: high	Нормализатор "Microsoft products" tags → description logsource DeviceVendor = Microsoft DeviceProduct = Windows DeviceEventClassID=4688 selection1: DestinationProcessName endswith '' DeviceCustomString4 contains "" OR DeviceCustomString4 contains "" Selection2 DestinationProcessName endswith '' DeviceCustomString4 contains "" OR DeviceCustomString4 contains "" selection3 DestinationProcessName endswith '' DeviceCustomString4 contains "" OR DeviceCustomString4 contains "" condition DeviceVendor = Microsoft AND DeviceProduct = Windows AND DeviceEventClassID=4688 AND ((DestinationProcessName endswith '' AND (DeviceCustomString4 contains "" OR DeviceCustomString4 contains "")) OR (DestinationProcessName endswith '' AND (DeviceCustomString4 contains "" OR DeviceCustomString4 contains "")) OR (DestinationProcessName endswith '' AND (DeviceCustomString4 contains "" OR DeviceCustomString4 contains ""))) identical fields – указывать поля из условия за исключением полей Name, deviceProduct, deviceVendor	DeviceVendor=' DeviceProduct= DeviceEventCla ((Destinati '\\wevtutil.ex (Devic DeviceCustomSt) OR ((Destin '\\powershell. Des '\\powershell\ '\\pwsh.exe') A (Device EventLog' OR D 'Remove-EventL) OR (Destinatio AND DeviceC 'ClearEventLog)

Правило Sigma	Сопоставление с объектами Kaspersky SIEM Cloud	

title: 0021-0002.1204.003 Execution - PowerExchangeDropper
description: Detect the dropping of PowerExchange components.
status: experimental
logsource:
  product: windows
  service: Sysmon
detection:
  selection1:
  EventID: 11
  selection2:
  TargetFilename|contains:
  - 'c:\users\public\microsoftedge\autosave.exe'
  - 'c:\users\public\microsoftedge\wsdl.ps1'
  selection3:
  Image|endswith: "brochure.exe"
  condition: selection1 and selection2 and selection3
falsepositives:
- Unknown
level: high
	Основание: Нормализатор 11 события Sysmon.
	title → name
	author → description
	description→ description
	status → description
	logsource
	DeviceVendor = Microsoft
	
	DeviceProduct = Sysmon
	
	selection1
	DeviceEventClassID=11
	selection2
	FilePath contains 'c:\users\public\microsoftedge\autosave.exe' OR FilePath contains ''
	
	если есть * пути к файлу форматировать в regexp
	selection3
	OldFilePath endswith ""
	condition:
	DeviceVendor = Microsoft AND
	
	DeviceProduct = Sysmon AND
	
	(DeviceEventClassID=11) AND (FilePath contains 'c:\users\public\microsoftedge\autosave.exe' OR FilePath contains '') AND (OldFilePath endswith "")
	identical fields – указывать поля из условия за исключением полей Name, deviceProduct, deviceVendor
	level →severity
	falsepositive → Description
		DeviceVendor='
		
		DeviceProduct=
		
		DeviceEventCla
		
		(
		
		  FilePath con
		'c:\\users\\pu
		OR
		
		  FilePath c
		'c:\\users\\pu
		
		) AND
		
		OldFilePath en

title: Domain joined host discovery description: Detect an attacker enumerating domain-joined machines using PowerShell. status: stable logsource: product: windows service: security detection: selection: EventID: 4104 ScriptBlockText|contains|all: - 'System.DirectoryServices.DirectorySearcher' - 'Properties.operatingsystem' condition: selection falsepositives: - "Administrative scripts or tools like Vulnerability Scanners" level: medium	ScriptBlockText → Message	

Правило Sigma	Сопоставление с объектами Kaspersky SIEM Cloud	
title: 0022-0002.1053.005 Execution - PowerExchange Task description: Detect the creation of a scheduled task by PowerExchange. status: experimental logsource: product: windows service: security detection: selection: EventID: - '4698' TaskName|contains: - 'MicrosoftEdgeUpdateService' condition: selection falsepositives: - Unknown level: medium	TaskName → SourceProcessName	

Правило Sigma	Сопоставление с объектами Kaspersky SIEM Cloud	
title: Created Windows Shell from Critical Windows Process description: Anomaly behavior critical windows process status: stable modified: 2023-07-18 tags: - attack.defense_evasion - attack.t1036 logsource: product: windows category: process_creation detection: selection: ParentImage|endswith: - '\searchindexer.exe' - '\lsaiso.exe' - '\lsm.exe' - '\spoolsv.exe' - '\wininit.exe' - '\smss.exe' - '\csrss.exe' - '\lsass.exe' - '\services.exe' - '\winlogon.exe' Image|endswith: - '\powershell_ise.exe' - '\cmstp.exe' - '\appvlp.exe' - '\mftrace.exe' - '\scriptrunner.exe' - '\forfiles.exe' - '\msiexec.exe' - '\rundll32.exe' - '\mshta.exe' - '\hh.exe' - '\wmic.exe' - '\regsvr32.exe' - '\scrcons.exe' - '\bash.exe' - '\sh.exe' - '\cscript.exe' - '\wscript.exe' - '\powershell.exe' - '\cmd.exe' condition: selection falsepositives: - Unknown level: high	ParentImage → SourceProcessName	

Правила сегментации

В Kaspersky SIEM Cloud можно настроить *правила сегментации алертов*, то есть правила разделения однотипных корреляционных событий по разным алертам.

По умолчанию, если в коррелляторе какое-то правило корреляции сработает несколько раз, все созданные в результате этого корреляционные события будут присоединены к одному алерту. Правила сегментации алертов дают возможность определить условия, при которых на основе таких однотипных корреляционных событий будут создаваться разные алерты. Это может пригодиться, если вы хотите разделить поток корреляционных событий, например, по количеству событий или объединить некоторых из событий, отличающиеся чем-то важным от других, в отдельный алерт.

Сегментация алертов настраивается в два этапа:

1. Создаются *правила сегментации*, в которых определяются условия, по которым будет разделяться поток корреляционных событий.

2. К правилам сегментации привязываются правила корреляции, в которых должны срабатывать правила сегментации.

Создание правила сегментации

Правила сегментации алертов используются для разделения однотипных корреляционных событий по разным алертам. Условия для корреляционных событий, по которым будут создаваться отдельные алерты, задаются в правилах сегментации.

Чтобы создать правило сегментации:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Правила сегментации**, выберите нужный тенант и нажмите на кнопку **Создать**.

2. В поле **Имя** укажите имя правила сегментации. Имя должно быть уникальным и содержать от 1 до 128 символов в кодировке Unicode.

3. При необходимости в раскрывающемся списке **Тенант** измените тенант, которому принадлежит правило сегментации.

4. В раскрывающемся списке **Тип** укажите тип правила сегментации. Доступные значения:

   - **По фильтру** – алерт создается, если корреляционные события соответствуют условиям фильтра, заданным в блоке параметров **Фильтр**.

     С помощью кнопки **Добавить условие** можно добавить строку с полями для определения условия. С помощью кнопки **Добавить группу** можно добавить группу фильтров. Можно переключать групповые операторы между **И**, **ИЛИ**, **НЕ**. В группы фильтров можно добавить другие группы условий и отдельные условия. Условия и группы можно менять местами, перетаскивая их с помощью значка ⣿, а также удалять с помощью значка ✕. Условия можно задать с помощью операндов и операторов:

     - Левый операнд и Правый операнд – используются для указания значений, которые будет обрабатывать оператор.

       В левом операнде указываются названия полей событий, которые обрабатывает фильтр.

       В правом операнде можно выбрать тип значения **константа** или **список**, а также указать само значение.

     - **Доступные операторы**

       - **=** – левый операнд равен правому операнду.

       - **<** – левый операнд меньше правого операнда.

- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.

Также можно добавить фильтр в режиме кода. Для этого необходимо перейти на вкладку **Код** в блоке **Фильтр** и в поле ввода указать параметры фильтра. При вводе значений параметров поддерживается автодополнение в виде списка подсказок с возможными вариантами значений. Для вызова списка всех подсказок в поле ввода используйте комбинацию клавиш **`Ctrl`** + **`Space`**.

> Обратите внимание, что режим кода позволяет использовать в списке подсказок все возможные значения для правил в Kaspersky SIEM Cloud. Некоторые из этих значений могут быть недопустимыми для правил сегментации (например, `activelist`, `dictionary`, `hasbit`).

- **По группирующим полям** – алерт создается, если корреляционное событие содержит поля событий, указанные в раскрывающемся списке **Группирующие поля правила корреляции**.

  Группирующие поля можно выбрать в раскрывающемся списке **Группирующие поля правила корреляции** с помощью флажков. Добавленные поля можно удалить, нажав на значок крестика около названия группирующего поля.

  Если вы выбрали несколько полей событий, алерт будет создаваться, если в корреляционном событии заполнено хотя бы одно из выбранных полей. При этом отдельный алерт будет создаваться для каждой уникальной комбинации полей корреляционного события. Например, если вы выбрали три поля: поле 1, поле 2 и поле 3, возможны следующие варианты создания алертов:

  - Заполнено поле 2, поля 1 и 3 пустые: создается алерт 1.
  - Заполнено поле 2, поля 1 и 3 пустые. Если значение поля 2 совпадает со значением поля 2 в алерте 1, то корреляционное событие будет добавлено к алерту 1. Если значения поля 2 не совпадают, то будет создан алерт 2.
  - Заполнено поле 3, поля 1 и 2 пустые: создается алерт 3.
  - Заполнены поля 2 и 3, поле 1 пустое: создается алерт 4, даже если значение поля 2 совпадает со значением поля 2 в алерте 1, а значение поля 3 совпадает со значением поля 3 в алерте 3.
  - Заполнены поля 1, 2 и 3: создается алерт 5.

  Пример использования группирующих полей

Правило, детектирующее сканирование сети, создаст только один алерт, даже если в сети есть несколько устройств, сканирующих сеть. Если создать правило сегментации алертов по группирующему полю событий `SourceAddress`, а затем привязать это правило сегментации к правилу корреляции, при срабатывании правила будут созданы алерты для каждого адреса, с которого происходит сканирование.

В этом примере, если правило корреляции называется "`Network. Possible port scan`", а в ресурсе правила сегментации в качестве шаблона именования алертов указано "`from {{.SourceAddress}}`", будут созданы алерты такого вида:

- `Network. Possible port scan (from 10.20.20.20)`
- `Network. Possible port scan (from 10.10.10.10)`

- **По количеству событий** – алерт создается, если количество корреляционных событий в предыдущем алерте превысило значение, указанное в поле **Количество корреляционных событий**.

5. В поле **Шаблон именования алертов** укажите шаблон, в соответствии с которым алерты, создаваемые по этому правилу сегментации, будут получать название. Значение по умолчанию: `{{.Timestamp}}`. В поле шаблона можно указывать текст, а также поля события в формате `{{.<название поля события>}}`. При формировании названия алерта вместо названия поля события будет подставляться его значение. Название алерта, созданного с помощью правил сегментации, имеет следующий формат: `<Name of the correlation rule that generated the alert> <text from the alert naming template field> <value of the specified event field>`. Например, если сработавшее правило корреляции называется "`Connection. Insecure port usage`" и в шаблоне наименования правила сегментации указано `{{.Timestamp}}`, будут созданы алерты вида:

   - `Connection. Insecure port usage (Tue, 29 Jul 2025 07:56:43 UTC)`
   - `Connection. Insecure port usage (Tue, 29 Jul 2025 07:59:46 UTC)`

   Если выполнится несколько правил сегментации с разными шаблонами именования алертов, в названии алерта они будут перечислены через разделительную черту `" | "`.

6. При необходимости в раскрывающемся списке **Теги** выберите теги для правила сегментации событий.

7. При необходимости в поле **Описание** укажите описание правила сегментации. Вы можете указать до 4000 символов в кодировке Unicode.

Правило сегментации будет создано. Далее созданное правило сегментации нужно связать с правилом корреляции.

Привязка правил сегментации к правилам корреляции

Связи правила сегментации и правил корреляции отображаются в разделе **Параметры** → **Алерты** → **Сегментация** веб-интерфейса Kaspersky SIEM Cloud в таблице со следующими столбцами:

- **Тенант** – название тенанта, которому принадлежат правила сегментации.
- **Обновлено** – дата и время последнего обновления правил сегментации.
- **Выключено** – в этом столбце отображается метка, если правила сегментации выключены.

Чтобы привязать правило сегментации алерта к правилам корреляции:

1. Откройте раздел **Параметры** → **Алерты** → **Сегментация** веб-интерфейса Kaspersky SIEM Cloud.
2. В блоке параметров **Связи правил сегментации** нажмите **Добавить** и укажите параметры правила сегментации:
   - **Название** (обязательно) – в этом поле укажите название правила сегментации. Должно содержать от 1 до 128 символов в кодировке Unicode.
   - **Правило сегментации** (обязательно) – в этом блоке параметров требуется выбрать ранее созданное правило сегментации, в котором определены условия сегментации.
   - **Выключено** – установите этот флажок при необходимости выключить связь правила сегментации.
3. Нажмите **Сохранить**.

   Правило сегментации и правила корреляции связаны. Корреляционные события, создаваемые указанными правилами корреляции, будут объединены в отдельный алерт с названием, определенном в правиле сегментации.

Чтобы выключить связи правил сегментации и правил корреляции:

1. Откройте раздел **Параметры** → **Алерты** веб-интерфейса Kaspersky SIEM Cloud и выберите тенант, правила сегментации которого вы хотите выключить.
2. Установите флажок **Выключено**.
3. Нажмите **Сохранить**.

   Связи правил сегментации и правил корреляции выключены.

Активные листы

Активный лист – это контейнер для данных, которые используются коррелятором Kaspersky SIEM Cloud при анализе событий по правилам корреляции.

Например, если у вас есть список IP-адресов с плохой репутацией, вы можете:

1. Создать правило корреляции типа operational и добавить в активный лист эти IP-адреса.
2. Создать правило корреляции типа standard и указать активный лист в качестве условия фильтрации.
3. Создать коррелятор с этим правилом.

   В этом случае Kaspersky SIEM Cloud выберет все события, которые содержат IP-адреса, внесенные в активный лист, и создаст корреляционное событие.

Вы можете наполнять активные листы автоматически с помощью правил корреляции типа simple или импортировать файл с данными для активного листа.

Вы можете добавлять, копировать и удалять активные листы.

Активные листы можно использовать в правилах корреляции и панелях мониторинга.

Один и тот же активный лист может использоваться в разных коррелляторах. При этом для каждого коррелятора создается своя сущность активного листа. Таким образом, содержимое активных листов, используемых разными коррелляторами, различается, даже если идентификатор и название активных листов одинаковые. Активный лист следует привязать к правилу корреляции, а правило корреляции привязать к коррелятору.

В активный лист добавляются данные только по правилам корреляции, добавленным в коррелятор.

Вы можете добавлять, изменять, дублировать, удалять и экспортировать записи в активном листе коррелятора.

> Если во время работы с данными активного листа коррелятор выключен, то в интерфейсе отображается ошибка "Internal communication failed", сообщающая о том, что потеряно соединение с источником данных, а именно потеряно соединение с коррелятором.

В процессе корреляции при удалении записей из активных листов по истечении срока жизни записи в коррелляторах создаются служебные события. Эти события существуют только в коррелляторах, они не перенаправляются в другие точки назначения. Правила корреляции можно настроить на отслеживание этих событий, чтобы обрабатывать эти события и с их помощью распознавать угрозы. Поля служебных событий удаления записи из активного листа описаны ниже.

Поле события	Значение или комментарий
`ID`	Идентификатор события.
`Timestamp`	Время удаления записи, срок жизни которой истек.
`Name`	`active list record expired`
`DeviceVendor`	`Kaspersky`
`DeviceProduct`	`Kaspersky SIEM Cloud`
`ServiceID`	Идентификатор коррелятора.
`ServiceName`	Название коррелятора.
`DeviceExternalID`	Идентификатор активного листа.
`DevicePayloadID`	Ключ записи, срок жизни которого истек.
`BaseEventCount`	Увеличенное на единицу количество обновлений удаленной записи.
`S.<поле активного листа>`	Выпавшая запись активного листа в формате: `S.<поле активного листа> = <значение активного листа>`

Просмотр таблицы активных листов коррелятора

Чтобы просмотреть таблицу активных листов коррелятора:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
2. Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.
3. В панели инструментов или в меню (⋮) нажмите **Смотреть активные листы**.

   Отобразится таблица **Активные листы коррелятора**.

Описание таблицы Активные листы коррелятора

Название столбца	Описание
Название	Название активного листа.
Записи	Количество записей в активном листе.
Размер на диске	Место, которое активный лист занимает на диске, КБ.
Каталог	Путь к активному листу на сервере коррелятора Kaspersky SIEM Cloud.

Добавление активного листа

Чтобы добавить активный лист:

1. В веб-консоли перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные листы**.
2. На панели инструментов или в меню (⋮) нажмите **Добавить активный лист**.
3. Выполните следующие действия:
   a. В поле **Название** введите название активного листа.
   b. В раскрывающемся списке **Тенант** укажите тенант, которому принадлежит ресурс.
   c. В поле **Срок жизни** укажите время в секундах, в течение которого в активном листе будет храниться добавленная в него запись.

      По истечении указанного времени запись удаляется. Время указывается в секундах. Значение по умолчанию: 0. Если в поле указано значение 0, запись хранится 36 000 дней.
   d. При необходимости в поле **Теги** укажите теги для поиска ресурса.
   e. При необходимости в поле **Описание** введите дополнительную информацию.

      Вы можете использовать до 4000 символов в кодировке Unicode.
4. Чтобы сохранить активный лист, выберите один из следующих вариантов:
   - Нажмите на кнопку **Сохранить**.
   - Нажмите на кнопку **Сохранить с комментарием**.

     При необходимости в появившемся окне **Оставить комментарий** добавьте комментарий. Чтобы просмотреть комментарии для активного листа, в таблице активных листов установите флажок рядом с нужным активным листом и на панели инструментов или в меню (⋮) нажмите **Показать историю версий**. В появившемся окне **История версий** будет отображаться таблица со списком доступных версий активного листа и вы сможете просмотреть комментарии.

Активный лист будет добавлен.

Просмотр параметров активного листа

Чтобы просмотреть параметры активного листа:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные листы**.

   Отобразится таблица доступных активных листов.

2. В столбце **Название** выберите активный лист, параметры которого вы хотите просмотреть.

Отобразятся параметры активного листа. См. описание параметров активного листа в следующей таблице.

Описание параметров активного листа

Название параметра	Описание
ID	Идентификатор активного листа.
Название	Уникальное название активного листа.
Тенант	Название тенанта, которому принадлежит активный лист.
Срок жизни	Время, в течение которого в активном листе будет храниться добавленная в него запись. Указывается в секундах.
Теги	Теги для поиска активного листа.
Описание	Любая дополнительная информация об активном листе.
Коррелятор	Имя коррелятора, к которому привязан активный лист. Поле отображается, если активный лист привязан к коррелятору.

Если активный лист привязан к коррелятору, отображается таблица значений активного листа.

Изменение параметров активного листа

Чтобы изменить параметры активного листа:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные листы**.

   Отобразится таблица доступных активных листов.

2. В столбце **Название** выберите активный лист, параметры которого вы хотите изменить.

3. Измените необходимые параметры:

   - **Название** – уникальное название активного листа.
   - **Срок жизни** – время в секундах, в течение которого в активном листе будет храниться добавленная в него запись.

     Если в поле указано значение 0, запись хранится 36 000 дней.
   - **Теги** – теги для поиска активного листа.
   - **Описание** – любая дополнительная информация об активном листе.

Параметры **ID**, **Тенант** и **Коррелятор** недоступны для редактирования.

Дублирование активного листа

Чтобы скопировать активный лист:

1. В веб-консоли перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные листы**.
2. Установите флажок рядом с активным листом, который вы хотите скопировать.
3. На панели инструментов или в меню (⋮), нажмите **Дублировать**.
4. Укажите название листа и тенант, в который вы хотите скопировать активный лист. По умолчанию активному листу, который вы дублируете, присваивается имя в формате <Название_активного_листа>-копия, а также он дублируется в тот тенант, в котором вы сейчас находитесь.
5. Чтобы сохранить активный лист, выберите один из следующих вариантов:
   - Нажмите на кнопку **Сохранить**.
   - Нажмите на кнопку **Сохранить с комментарием**.

     При необходимости в появившемся окне **Оставить комментарий** добавьте комментарий. Чтобы просмотреть комментарии для активного листа, в таблице активных листов установите флажок рядом с нужным активным листом и на панели инструментов или в меню (⋮) нажмите **Показать историю версий**. В появившемся окне **История версий** будет отображаться таблица со списком доступных версий активного листа и вы сможете просмотреть комментарии.

Активный лист будет скопирован.

Удаление активных листов

Чтобы удалить активные листы:

1. В веб-консоли перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные листы**.
2. В списке установите флажки рядом с активными листами, которые вы хотите удалить.

   Если вы хотите удалить все активные листы, установите флажок рядом со столбцом **Название** и в отобразившемся контекстном меню выберите одну из следующих опций:
   - **Выбрать все**.
   - **Выбрать все на странице**.

   Должен быть установлен хотя бы один флажок.
3. Нажмите на кнопку **Удалить**.

4. В окне подтверждения нажмите **Удалить**.

   Если на выбранные активные листы есть ссылки из других ресурсов и сервисов, удаление будет недоступно. В таком случае необходимо сначала отвязать активные листы от корреляционных правил и коррелляторов.

Активные листы будут удалены.

Просмотр записей в активном листе

Чтобы просмотреть список записей в активном листе:

1. В веб-консоли выполните одно из следующих действий:

   - Перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные листы**.

     Отобразится таблица доступных активных листов.

   - Перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.

     В списке установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист. На панели инструментов или в меню (⋮) нажмите **Смотреть активные листы**.

     Отобразится таблица **Активные листы коррелятора**.

2. В столбце **Название** выберите нужный вам активный лист.

Откроется таблица записей для выбранного активного листа. Если активный лист привязан к коррелятору, отображается таблица значений активного листа.

Описание таблицы записей активного листа

Название параметра	Описание
Ключ	Название ключа активного листа. Можно указать несколько значений, используя символ |.
Значение	Значение ключа активного листа. Можно указать несколько значений ключа через запятую в формате JSON.
Действия	Действия, доступные с записями активного листа. Вы можете изменять или удалять записи.
Повторы записи	Общее количество упоминаний записи в событиях и загрузок идентичных записей при импорте активных листов в Kaspersky SIEM Cloud.
Срок действия	Дата и время, когда запись будет удалена. Если при создании активного листа в поле **Срок жизни** было указано значение 0, записи этого активного листа хранятся 36 000 дней.
Последнее обновление	Время последнего обновления активного листа.

На странице отображается не более 64 строк активного листа. При необходимости вы можете прокрутить страницу, чтобы просмотреть все строки.

Поиск записей в активном листе

Чтобы найти запись в активном листе:

1. В веб-консоли выполните одно из следующих действий:

   - Перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные листы**.

     Отобразится таблица доступных активных листов.

- Перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.

  Установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист. На панели инструментов или в меню (⋮) нажмите **Смотреть активные листы**.

  Отобразится таблица **Активные листы коррелятора**.

2. В столбце **Название** выберите нужный вам активный лист.

   Откроется таблица записей выбранного активного листа.

3. В поле **Поиск** введите название ключа записи или несколько символов из названия. Также вы можете выполнить поиск по значению ключа.

В таблице записей активного листа отобразятся только те записи, в значении которых есть введенные символы.

Добавление записи в активный лист

Чтобы добавить запись в активный лист:

1. В веб-консоли выполните одно из следующих действий:

   - Перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные листы**.

     Отобразится таблица доступных активных листов.

   - Перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.

     В списке установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист. На панели инструментов или в меню (⋮) нажмите **Смотреть активные листы**.

     Отобразится таблица **Активные листы коррелятора**.

2. В столбце **Название** выберите нужный вам активный лист.

   Откроется таблица записей для выбранного активного листа.

3. Нажмите на кнопку **Добавить**.

4. Укажите значения для следующих параметров:

   a. В поле **Ключ** введите имя записи.

      Вы можете указать несколько значений, используя символ |.

   b. В поле **Значение** укажите значение в формате JSON. Вы можете указать несколько значений.

5. Нажмите на кнопку **Сохранить**.

Запись будет добавлена. После сохранения записи в активном листе будут отсортированы в алфавитном порядке.

На странице доступно для отображения не более 64 строк активного листа. При необходимости вы можете прокрутить страницу, чтобы просмотреть все строки.

Дублирование записей в активном листе

Чтобы дублировать запись в активном листе:

1. В веб-консоли выполните одно из следующих действий:

   - Перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные листы**.

     Отобразится таблица доступных активных листов.

   - Перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.

     В списке установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист. На панели инструментов или в меню (⋮) нажмите **Смотреть активные листы**.

     Отобразится таблица **Активные листы коррелятора**.

2. В столбце **Название** выберите нужный вам активный лист.

   Откроется таблица записей для выбранного активного листа.

3. Установите флажок рядом с записью, которую вы хотите скопировать.

4. Нажмите на кнопку **Дублировать**.

5. Укажите ключ и при необходимости измените значения ключа.

6. Нажмите на кнопку **Сохранить**.

   Запись будет скопирована. После сохранения записи в активном листе будут отсортированы в алфавитном порядке.

На странице доступно для отображения не более 64 строк активного листа. При необходимости вы можете прокрутить страницу, чтобы просмотреть все строки.

Изменение записи в активном листе

Чтобы изменить запись в активном листе:

1. В веб-консоли выполните одно из следующих действий:

   - Перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные листы**.

     Отобразится таблица доступных активных листов.

   - Перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.

     В списке установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист.

     На панели инструментов или в меню (⋮) нажмите **Смотреть активные листы**. Отобразится таблица **Активные листы коррелятора**.

2. В столбце **Название** выберите нужный вам активный лист.

   Откроется таблица записей для выбранного активного листа.

3. Нажмите на значок карандаша в столбце **Действия**.

4. Измените требуемые значения ключа в формате JSON.

5. Если вы хотите подтвердить изменения, нажмите на галочку в столбце **Действия**. Если вы хотите отменить изменения, нажмите на значок крестика в столбце **Действия**.

6. Нажмите **Сохранить**.

Запись будет изменена. После сохранения записи в активном листе будут выстроены в алфавитном порядке.

На странице доступно для отображения не более 64 строк активного листа. При необходимости вы можете прокрутить страницу, чтобы просмотреть все строки.

Удаление записей в активном листе

Чтобы удалить записи из активного листа:

1. В веб-консоли выполните одно из следующих действий:

   - Перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные листы**.

     Отобразится таблица доступных активных листов.

   - Перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.

     В списке установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист. На панели инструментов или в меню (⋮) нажмите **Смотреть активные листы**. Отобразится таблица **Активные листы коррелятора**.

2. В столбце **Название** выберите нужный вам активный лист.

   Откроется таблица записей для выбранного активного листа.

3. Установите флажки рядом с записями, которые вы хотите удалить.

   Если вы хотите удалить все записи, установите флажок рядом с названием столбца **Ключ**.

   > Должен быть установлен хотя бы один флажок.

4. Нажмите на кнопку **Удалить**.

5. Нажмите на кнопку **OK**.

Записи будут удалены.

На странице доступно для отображения не более 64 строк активного листа. При необходимости вы можете прокрутить страницу, чтобы просмотреть все строки.

Импорт записей в активный лист

Чтобы импортировать записи в активный лист:

1. В веб-консоли выполните одно из следующих действий:

   - Перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные листы**.

     Отобразится таблица доступных активных листов. Нажмите на название активного листа и в открывшемся окне **Редактирование активного листа** в секции **Контент** установите флажки рядом с записями, которые вы хотите импортировать.

   - Перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.

     В списке установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист. На панели инструментов или в меню (⋮) нажмите **Смотреть активные листы**.

     В отобразившейся таблице **Активные листы коррелятора** установите флажок рядом с требуемым активным листом.

2. В панели инструментов нажмите **Импортировать**.

   Откроется окно импорта активного листа.

3. Нажмите на кнопку **Добавить** и в открывшемся окне выберите файл, который требуется импортировать.

4. В раскрывающемся списке **Формат** выберите формат файла:

   - **csv**;
   - **tsv**;
   - **internal**.

     Активный лист должен быть в формате JSON.

5. В поле **Ключевое поле** введите название столбца с ключами записей активного листа, который указан в файле. Поле недоступно для формата **internal**.

6. Нажмите на кнопку **Импортировать**.

Данные из файла будут импортированы в активный лист. Записи, внесенные в лист ранее, сохраняются.

При импорте данные из файла не проходят проверку на допустимые символы. Если вы будете использовать эти данные в виджетах, при наличии недопустимых символов в данных виджеты будут отображаться некорректно.

Экспорт записей из активного листа

Чтобы экспортировать записи активного листа:

1. В веб-консоли выполните одно из следующих действий:

   - Перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные листы**.

     Отобразится таблица доступных активных листов. Нажмите на название активного листа и в открывшемся окне **Редактирование активного листа** в секции **Контент** установите флажки рядом с записями, которые вы хотите экспортировать.

   - Перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**.

     В списке установите флажок напротив коррелятора, для которого вы хотите просмотреть активный лист. В панели инструментов или в меню ⋮ нажмите **Смотреть активные листы**.

     В отобразившейся таблице **Активные листы коррелятора** установите флажок рядом с требуемым активным листом.

2. В панели инструментов нажмите **Экспортировать**.

Активный лист будет загружен в формате JSON в папку по умолчанию или в папку, указанную в параметрах вашего браузера. Название загруженного файла соответствует названию активного листа.

Предустановленные активные листы

В поставку Kaspersky SIEM Cloud включены перечисленные в таблице ниже активные листы.

Предустановленные активные листы

Название активного листа	Описание
[OOTB][AD] End-users tech support accounts	Активный список используется в качестве фильтра при работе корреляционного правила [OOTB][AD] Successful authentication with same user account on multiple hosts. В активный список могут быть добавлены учетные записи сотрудников технической поддержки. Записи не удаляются из активного списка.
[OOTB][AD] List of sensitive groups	Активный список используется в качестве фильтра при работе корреляционного правила [OOTB][AD] Membership of sensitive group was modified. В активный список могут быть добавлены критичные доменные группы, членство в которых необходимо отслеживать. Записи не удаляются из активного списка.
[OOTB][Linux] CompromisedHosts	Активный список наполняется правилом [OOTB] Successful Bruteforce потенциально скомпрометированными хостами под управлением ОС Linux. Записи удаляются из списка через 24 часа после внесения.
[OOTB][Net] Detection unknown assets	Активный список используется в качестве стоп-листа при работе корреляционных правил: [OOTB][Net] Detection unknown assets in source fields, [OOTB][Net] Detection unknown assets in destination fields, [OOTB][Net] Detection unknown assets in device fields.

Контекстные таблицы

Контекстная таблица – это контейнер для массива данных, которые используются коррелляторами Kaspersky SIEM Cloud при анализе событий по правилам корреляции. Вы можете создать контекстные таблицы в разделе **Мониторинг** → **Ресурсы и сервисы**. Данные контекстной таблицы хранятся только в корреляторе, в который она была добавлена с помощью фильтров или действий в корреляционных правилах.

Вы можете наполнять контекстные таблицы автоматически с помощью корреляционных правил типа simple и operational или импортировать файл с данными для контекстной таблицы.

Вы можете добавлять, копировать и удалять контекстные таблицы, а также изменять их настройки.

Контекстные таблицы можно использовать в следующих сервисах и функциях Kaspersky SIEM Cloud:

- Правила корреляции.
- Панель мониторинга.

Одна и та же контекстная таблицы может использоваться в разных коррелляторах. При этом для каждого коррелятора создается своя сущность контекстной таблицы. Таким образом, содержимое контекстных таблиц, используемых разными корреляторами, различается, даже если идентификатор и название контекстных таблиц одинаковые.

В контекстную таблицу добавляются данные только по правилам корреляции, добавленным в коррелятор.

Вы можете добавлять, изменять, удалять, импортировать и экспортировать записи в контекстной таблице коррелятора.

> Если во время работы с данными контекстной таблицы коррелятор выключен, то в интерфейсе отображается ошибка "Internal communication failed", сообщающая о том, что потеряно соединение с источником данных, а именно потеряно соединение с коррелятором.

При удалении записей из контекстных таблиц по истечении срока жизни записи в корреляторах создаются служебные события. Эти события существуют только в корреляторах, они не перенаправляются в другие точки назначения. Служебные события отправляются на обработку правилами корреляции того коррелятора, где работает контекстная таблица. Правила корреляции можно настроить на отслеживание этих событий, чтобы с их помощью обрабатывать события и распознавать угрозы.

Поля служебных событий удаления записи из контекстной таблицы описаны ниже.

Поле события	Значение или комментарий
`ID`	Идентификатор события.
`Timestamp`	Время удаления записи, срок жизни которой истек.
`Name`	`context table record expired`
`DeviceVendor`	`Kaspersky`
`DeviceProduct`	`Kaspersky SIEM Cloud`
`ServiceID`	Идентификатор коррелятора.
`ServiceName`	Название коррелятора.
`DeviceExternalID`	Идентификатор контекстной таблицы.
`DevicePayloadID`	Ключ записи, срок жизни которой истек.
`BaseEventCount`	Увеличенное на единицу количество обновлений удаленной записи.
`FileName`	Имя контекстной таблицы.

Поле события	Значение или комментарий

`S.<поле контекстной таблицы>`
`SA.<поле контекстной таблицы>`
`N.<поле контекстной таблицы>`
`NA.<поле контекстной таблицы>`
`F.<поле контекстной таблицы>`
`FA.<поле контекстной таблицы>`
	В зависимости от типа выпавшей записи в контекстной таблице, выпавшая запись контекстной таблицы будет записана в соответствующий тип события:
	`S.<поле контекстной таблицы> = <значение контекстной таблицы>`
	`SA.<поле контекстной таблицы> = <массив значений контекстной таблицы>`
	Записи контекстной таблицы типа boolean имеют следующий вид:
	`S.<поле контекстной таблицы> = true/false`
	`SA.<поле контекстной таблицы> = false,true,false`

Просмотр списка контекстных таблиц

Вы можете просмотреть полный список контекстных таблиц или список контекстных таблиц, привязанных к конкретному коррелятору.

Полный список контекстных таблиц

Чтобы просмотреть полный список контекстных таблиц,

в веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Контекстные таблицы**.

Отобразится список **Контекстные таблицы**.

Список контекстных таблиц конкретного коррелятора

Чтобы просмотреть список контекстных таблиц коррелятора:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
2. Установите флажок напротив коррелятора, для которого вы хотите просмотреть список контекстных таблиц.
3. В панели инструментов или в меню (⋮) нажмите **Смотреть контекстные таблицы**.

   Отобразится список **Контекстные таблицы коррелятора**.

Таблица содержит следующие данные:

- **Название** – имя контекстной таблицы.
- **Записи** – количество записей в контекстной таблице.
- **Размер на диске** – размер контекстной таблицы.
- **Директория** – путь к контекстной таблице на сервере коррелятора Kaspersky SIEM Cloud.

Добавление контекстной таблицы

Чтобы добавить контекстную таблицу:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Контекстные таблицы**.
2. В окне **Контекстные таблицы** нажмите на кнопку **Создать**.

   Откроется окно **Создание контекстной таблицы**.
3. В поле **Название** введите имя контекстной таблицы.
4. В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит ресурс.
5. В поле **Срок жизни** укажите время, в течение которого в контекстной таблице будет храниться добавленная в него запись.

   По истечении указанного времени запись удаляется. Время указывается в секундах. Максимальное значение – `31536000` (1 год).

   Значение по умолчанию: `0`. Если в поле указано значение 0, время хранения записи неограниченно.
6. В раскрывающемся списке **Теги** выберите теги для создаваемой контекстной таблицы.

   В списке отображаются все доступные теги, созданные в тенанте ресурса и Общем тенанте. Вы можете найти тег в списке, начав вводить его название в поле. Если тега, который вы ввели, не существует, вы можете нажать **`Enter`** или **Добавить**, чтобы создать его.
7. В поле **Описание** введите любую дополнительную информацию.

   Вы можете использовать до 4000 символов в кодировке Unicode.

   Поле необязательно для заполнения.
8. На вкладке **Схема** укажите состав полей контекстной таблицы и тип данных полей.

   В зависимости от типа данных поле может быть или не быть ключевым. Хотя бы одно поле таблицы должно быть ключевым. Имена у всех полей должны быть уникальными.

   Для добавления строки таблицы нажмите на кнопку **Добавить** и заполните поля таблицы:

   a. В поле **Название** введите название поля. Максимальная длина – 128 символов.

   b. В раскрывающемся списке **Тип** выберите тип данных поля.

   Возможные типы данных поля

   Возможные типы данных поля контекстной таблицы

Тип данных поля	Может быть ключевым полем	Комментарий
Целое число	Да	—
Число с плавающей точкой	Да	—
Строка	Да	—
Логический тип	Да	—
Временная метка	Да	Для поля этого типа проверяется, что значение поля больше или равно нулю. Другие операции не предусмотрены.
IP-адрес	Да	Для поля этого типа проверяется, что значение поля соответствует формату IPv4, IPv6. Другие операции не предусмотрены.

Тип данных поля	Может быть ключевым полем	Комментарий
Список целых чисел	Нет	—
Список чисел с плавающей точкой	Нет	—
Список строк	Нет	—
Список логических типов	Нет	—
Список временных меток	Нет	Для поля этого типа проверяется, что каждый элемент списка больше или равен нулю. Другие операции не предусмотрены.
Список IP-адресов	Нет	Для поля этого типа проверяется, что каждый элемент списка соответствует формату IPv4, IPv6. Другие операции не предусмотрены.

c. Если вы хотите сделать поле ключевым, установите флажок **Ключевое поле**.

В таблице может быть несколько ключевых полей. Ключевые поля задаются при создании контекстной таблицы, уникально идентифицируют запись таблицы и не могут изменяться.

Если ключевых полей в контекстной таблице несколько, каждая запись таблицы уникально идентифицируется несколькими полями (составной ключ).

9. Добавьте нужное количество строк контекстной таблицы.

После сохранения контекстной таблицы изменить количество строк невозможно.

10. Нажмите на кнопку **Создать**.

Контекстная таблица будет добавлена.

После добавления контекстной таблицы привяжите ее к правилу корреляции в параметрах правила корреляции в разделе **Обновление контекстных таблиц**. Затем привяжите это правило корреляции к коррелятору. После привязки правила корреляции к коррелятору в параметрах контекстной таблицы появится поле **Коррелятор** и раздел **Контент**, в котором вы можете работать с содержимым контекстной таблицы.

Просмотр параметров контекстной таблицы

Чтобы просмотреть параметры контекстной таблицы:

1. В веб-консоли перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Контекстные таблицы**.

2. В списке выберите контекстную таблицу, параметры которой вы хотите просмотреть.

Откроется окно с параметрами контекстной таблицы. В нем отображается следующая информация:

- **Название** – уникальное имя ресурса.
- **Тенант** – название тенанта, которому принадлежит ресурс.
- **Срок жизни** – время, в течение которого в контекстной таблице будет храниться добавленная в нее запись. Указывается в секундах.

- **Описание** – любая дополнительная информация о ресурсе.
- **Схема** – упорядоченный список полей и их типов данных с отметкой ключевых полей.

Изменение параметров контекстной таблицы

Чтобы изменить параметры контекстной таблицы:

1. В веб-консоли перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Контекстные таблицы**.
2. В списке выберите контекстную таблицу, параметры которой вы хотите изменить.
3. Укажите значения для следующих параметров:
   - **Название** – уникальное имя ресурса.
   - **Тенант** – тенант, которому принадлежит ресурс. Это поле недоступно для редактирования.
   - **Срок жизни** – время, в течение которого в контекстной таблице будет храниться добавленная в нее запись. Указывается в секундах.
   - **Теги** – теги для поиска ресурса.
   - **Описание** – любая дополнительная информация о ресурсе.
   - **Коррелятор** – коррелятор, к которому привязано правило корреляции, в котором используется контекстная таблица. Это поле недоступно для изменения. Это поле появляется после привязки правила корреляции к коррелятору.
   - **Контент** – содержимое контекстной таблицы. Этот раздел появляется после привязки правила корреляции к коррелятору.

     Как менять содержимое контекстной таблицы

     Чтобы наполнить контекстную таблицу вручную или поменять ее содержимое, вам доступны следующие операции:

     - Добавить, изменить или удалить строку в таблице.
     - Дублировать строку.

       Вместо создания новой строки вы можете дублировать выбранную строку, изменить значения полей и сохранить.

     - Экспортировать контекстную таблицу.
     - Импортировать контекстную таблицу.
4. Перейдите на вкладку **Схема**. На этой вкладке отображается упорядоченный список полей и их типов данных с отметкой ключевых полей. Если контекстная таблица не используется в корреляционном правиле, вы можете поменять состав полей.

   Если вы хотите изменить схему в контекстной таблице, которая уже используется в корреляционном правиле, выполните шаги инструкции ниже.
5. Нажмите **Сохранить**.

Чтобы изменить параметры контекстной таблицы, ранее используемой коррелятором:

1. Выполните экспорт данных из таблицы.
2. Скопируйте и сохраните путь к файлу с данными таблицы на диске коррелятора. Путь указан в столбце **Директория** в окне **Контекстные таблицы коррелятора**. Этот путь понадобится вам в дальнейшем для удаления файла с диска коррелятора.
3. Удалите из коррелятора контекстную таблицу.
4. Измените необходимые параметры контекстной таблицы.
5. Удалите файл с данными таблицы на диске коррелятора по пути из шага 2.
6. Чтобы применить изменения (удаление таблицы), обновите параметры коррелятора: в разделе **Мониторинг → Ресурсы и сервисы → Активные сервисы** в списке сервисов установите флажок рядом с нужным коррелятором и нажмите **Обновить параметры**.
7. Добавьте в коррелятор контекстную таблицу, в которой вы изменили параметры.
8. Чтобы применить изменения (добавление таблицы), обновите параметры коррелятора: в разделе **Мониторинг → Ресурсы и сервисы → Активные сервисы** в списке сервисов установите флажок рядом с нужным коррелятором и нажмите **Обновить параметры**.
9. Адаптируйте в экспортированной таблице (см. шаг 1) поля, чтобы они соответствовали полям таблицы, которую вы загрузили в коррелятор на шаге 7.
10. Импортируйте адаптированные данные в контекстную таблицу.

Параметры контекстной таблицы изменены.

Дублирование параметров контекстной таблицы

Чтобы скопировать контекстную таблицу:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Контекстные таблицы**.
2. В списке установите флажок рядом с контекстной таблицей, которую вы хотите копировать.
3. Нажмите на кнопку **Дублировать**.
4. Измените значения нужных параметров.
5. Нажмите на кнопку **Сохранить**.

Контекстная таблица будет скопирована.

Удаление контекстной таблицы

Вы можете удалить только те контекстные таблицы, которые не используются ни в одном в корреляторе.

Чтобы удалить контекстную таблицу:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Контекстные таблицы**.
2. В списке установите флажки рядом с контекстными таблицами, которые вы хотите удалить.

   Если вы хотите удалить все контекстные таблицы, установите флажок рядом со столбцом **Название**.

   > Должен быть установлен хотя бы один флажок.

3. Нажмите на кнопку **Удалить**.
4. Нажмите на кнопку **ОК**.

Контекстные таблицы будут удалены.

Просмотр и поиск записей контекстной таблицы

Чтобы просмотреть список записей контекстной таблицы:

1. Перейдите к полному списку контекстных таблиц или к списку контекстных таблиц конкретного коррелятора.
2. Выберите нужную контекстную таблицу.

   Откроется список записей для выбранной контекстной таблицы.

   Для поиска по таблице в поле **Поиск** введите значение ключа записи или значение поля. В списке записей контекстной таблицы отобразятся только те записи, в которых есть введенные символы.

   Если под условие вашего поискового запроса попадают записи с пустыми значениями в ключе, в разделе **Панель мониторинга** на виджете отобразится текст <По вашему запросу ничего не найдено>. Мы рекомендуем уточнить условия поискового запроса.

Список записей содержит следующие данные:

- **Ключ** – композитный ключ записи. Формируется из одного и более значений ключевых полей, разделенных символом "|". Если одно из значений ключевого поля отсутствует, то разделяющий символ все равно отображается.

  Например, ключ записи состоит из трех полей: `DestinationAddress`, `DestinationPort`, `SourceUserName`. При отсутствии значений в последних двух полях ключ записи будет отображаться следующим образом: `43.65.76.98| |`.

- **Повторы записи** – общее количество упоминаний записи в событиях и загрузок идентичных записей при импорте контекстных таблиц в Kaspersky SIEM Cloud.
- **Срок действия** – дата и время, когда запись должна быть удалена. Формат даты и времени зависит от выбранного языка интерфейса решения.

  Если при создании контекстной таблицы в поле **Срок действия** было указано значение 0, записи этой контекстной таблицы хранятся 36 000 дней.

- **Последнее обновление** – дата и время обновления контекстной таблицы.

Добавление, изменение и удаление записей в контекстной таблице

Чтобы изменить содержимое контекстной таблицы:

1. Откройте контекстную таблицу, строки которой вы хотите изменить.

2. Выполните одно из следующих действий:

   - Если вы хотите добавить строку, нажмите на кнопку **Добавить** и укажите значения полей. Сохраните изменения, нажав на значок галочки (✓). Поля, указанные на вкладке **Схема** как ключевые, обязательны для заполнения.

     Kaspersky SIEM Cloud подставляет названия полей из правил корреляции, к которым привязана контекстная таблица. Эти названия недоступны для изменения. Состав полей изменить невозможно.

     Если вы укажете не все значения полей, отсутствующие поля будут заполнены значениями по умолчанию. Из итоговой совокупности полей будет сформирован ключ записи, и запись будет добавлена в таблицу. Если такой ключ в таблице уже существует, отобразится ошибка.

     Список значений полей по умолчанию

Тип поля	Значение по умолчанию
Целое число	0
Число с плавающей точкой	0.0
Строка	""
Логический тип	false
IP-адрес	"0.0.0.0"
Временная метка	0
Список целых чисел	[]
Список чисел с плавающей точкой	[]
Список строк	[]
Список логических типов	[]
Список временных меток	[]
Список IP-адресов	[]

     Если вы хотите изменить строку, в столбце **Действия** нажмите на значок карандаша (✎) и укажите значения полей. Сохраните изменения, нажав на значок галочки (✓).

     Значение полей типов **Временная метка** и **Список временных меток** должно быть больше или равно 0. Значение полей типов **IP-адрес** и **Список IP-адресов** должно соответствовать формату IPv4 или IPv6.

   - Если вы хотите дублировать строку, выделите строку, нажмите на кнопку **Дублировать** и укажите значения полей. Сохраните изменения, нажав на значок галочки (✓).

   - Если вы хотите удалить строку, в столбце **Действия** нажмите на значок корзины (🗑). Сохраните изменения, нажав на значок галочки (✓).

Контекстная таблица изменена.

Экспорт данных из контекстной таблицы

Чтобы экспортировать данные из контекстной таблицы:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
2. Выберите коррелятор, контекстную таблицу которого вы хотите экспортировать, и в панели инструментов или в меню (⋮) нажмите **Смотреть контекстные таблицы**.

   Откроется окно **Контекстные таблицы коррелятора**.
3. Установите флажок рядом с контекстной таблицей, которую нужно экспортировать.

   Вы не можете экспортировать несколько контекстных таблиц одновременно. Каждую таблицу нужно экспортировать отдельно.
4. Нажмите на кнопку **Экспортировать** и в раскрывающемся списке **Формат** выберите нужный формат:

   - **internal**.

     Контекстная таблица будет экспортирована в формате JSON.
   - **csv**.
   - **tsv**.
5. Нажмите на кнопку **Экспортировать**.

   Контекстная таблица будет загружена на ваше устройство в выбранном формате. Название экспортированного файла формируется по шаблону: <название_контекстной_таблицы>_<дата выгрузки (ГГГГ-ММ-ДД)>_<время выгрузки (ЧЧ-ММ-СС)>. При экспорте данные в файле сортируются по столбцу **Ключ**.

При экспорте в формате JSON (**internal**):

- Порядок столбцов в файле не определен.
- Поля с типом массив экспортируются в файл в виде массива значений, например: `["val1","val2","val3","val4"]`.
- Формат даты и времени в поле с типом **Временная метка** зависит от выбранного языка интерфейса решения.

При экспорте в форматах CSV и TSV:

- В первой строке файла указываются названия полей, строки ниже содержат данные.
- Для формата CSV в качестве разделителя полей используется запятая, а для формата TSV – знак табуляции.

Вы также можете экспортировать данные из контекстной таблицы в окне изменения параметров контекстной таблицы.

Импорт данных в контекстную таблицу

Чтобы импортировать данные в контекстную таблицу:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
2. В контекстном меню коррелятора, в контекстную таблицу которого вы хотите импортировать данные, выберите пункт **Смотреть контекстные таблицы**.

   Откроется окно **Контекстные таблицы коррелятора**.
3. Установите флажок рядом с нужной контекстной таблицей и нажмите на кнопку **Импортировать**.

   Откроется окно импорта данных в контекстную таблицу.
4. Нажмите **Добавить** и выберите файл, который требуется импортировать.
5. В раскрывающемся списке **Формат** выберите формат файла:

   - **csv**.
   - **tsv**.
   - **internal**.

     Контекстная таблица должна быть в формате JSON.
6. Нажмите на кнопку **Импортировать**.

   Данные из файла будут импортированы в контекстную таблицу. Записи, внесенные в контекстную таблицу ранее, сохраняются.

При импорте Kaspersky SIEM Cloud проверяет уникальность ключа каждой записи. Если запись уже существует, то в ее поля записываются новые значения, полученные слиянием прежних значений со значениями полей импортируемой записи.

Если записи в контекстной таблице не существовало, создается новая запись.

> При импорте данные из файла не проходят проверку на допустимые символы. Если вы будете использовать эти данные в виджетах, при наличии недопустимых символов в данных виджеты будут отображаться некорректно.

Вы также можете импортировать данные в контекстную таблицу в окне изменения параметров контекстной таблицы.

Обогащение событий

Обогащение событий – это дополнение событий информацией, которая может быть использована для выявления инцидента и при проведении расследования.

Обогащение выполняется с помощью *правил обогащения*. Правила обогащения позволяют добавлять в поля события дополнительную информацию путем преобразования данных, уже размещенных в полях, или с помощью запроса данных из внешних систем. Например, в событии есть имя учетной записи пользователя. С помощью правила обогащения вы можете добавить сведения об отделе, должности и руководителе этого пользователя в поля события.

Правила обогащения можно использовать в коллекторах, корреляторах и нормализаторах.

Если вы создаете правила обогащения в коллекторе и/или корреляторе, такие правила обогащения доступны для переиспользования. Также вы можете привязать к коллектору и/или коррелятору отдельно созданное правило обогащения.

Правила обогащения, созданные в нормализаторе, привязываются только к нормализатору и недоступны для переиспользования.

В комплект поставки решения входит предустановленное правило обогащения **[OOTB] EDR. Asset enrichment for collector**. Это правило обогащения позволяет настроить обогащение событий данными об активах на уровне коллектора.

Предустановленные правила обогащения можно удалить, но невозможно изменить.

Просмотр правил обогащения

Чтобы просмотреть правила обогащения:

1. В веб-интерфейсе откройте раздел **Мониторинг → Ресурсы и сервисы → Правила обогащения**.

   Откроется таблица правил обогащения.

   Правила обогащения можно искать по названию с помощью поля **Поиск**. При поиске правил обогащения используются регулярные выражения.

   Таблицу можно сортировать по названию, времени последнего обновления и по названию пакета, нажав на значок сортировки ⌄ в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

2. Если вы хотите просмотреть свойства конкретного правила обогащения, нажмите на это правило обогащения.

   Откроется окно с заданными значениями параметров правила обогащения. При необходимости вы можете изменить правило обогащения.

Создание правила обогащения

Чтобы создать правило обогащения событий:

1. В веб-интерфейсе откройте один из следующих разделов:

   - **Мониторинг → Ресурсы и сервисы → Правила обогащения**.
   - **Мониторинг → Ресурсы и сервисы → Список**.

2. В панели инструментов или в меню ⋮ нажмите на кнопку **Создать**.

3. В открывшейся боковой панели в поле **Название** введите уникальное имя правила обогащения. Название должно содержать от 1 до 128 символов в кодировке Unicode.

4. В раскрывающемся списке **Тип источника данных** выберите тип правила обогащения и настройте параметры, специфичные для выбранного типа источника данных:

   константа

   Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения описаны в таблице ниже.

   Параметры типа обогащения "константа"

Параметр	Описание
Константа	Значение, которое требуется добавить в поле события. Максимальная длина значения – до 255 символов в кодировке Unicode. Если оставить поле пустым, существующее значение поля события будет удалено.
Целевое поле	Поле события, в которое требуется поместить данные.

   Если вы используете функции обогащения событий для полей расширенной схемы с типом `Строка`, `Число` или `Число с плавающей точкой` с помощью константы, в поле будет добавлена константа.

   Если вы используете функции обогащения событий для полей расширенной схемы с типом `Массив строк`, `Массив чисел` или `Массив чисел с плавающей точкой` с помощью константы, константа будет добавлена к элементам массива.

   словарь

   Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Словарь**. Параметры этого типа обогащения описаны в таблице ниже.

   Параметры типа обогащения "словарь"

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.

   Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **словарь**, а в параметре **Ключевые поля обогащения** указано поле-массив, при передаче массива в качестве ключа словаря массив будет сериализован в строку в соответствии с правилами сериализации одного значения в формате TSV.

   Пример. В параметре **Ключевые поля обогащения** используется поле расширенной схемы `SA.StringArrayOne`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`. В качестве ключа в словарь будут переданы значения `['a','b','c']`.

   Если в параметре **Ключевые поля обогащения** используется поле-массив расширенной схемы и обычное поле схемы событий, значения полей при обращении в словарь будут разделены символом `|`.

   Пример. В параметре **Ключевые поля обогащения** используется поле расширенной схемы `SA.StringArrayOne` и строковое поле `Code`. В поле расширенной схемы `SA.StringArrayOne` находятся значения `"a"`, `"b"`, `"c"`, а строковое поле `Code` содержит последовательность символов `myCode`. В качестве ключа в словарь будут переданы значения `['a','b','c']|myCode`.

   событие

   Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры типа обогащения описаны в таблице ниже.

Параметры типа обогащения "событие"

Параметр	Описание
Целевое поле	Поле события, в которое следует поместить данные.
Исходное поле	Поле события, значение которого будет записано в целевое поле.
Преобразование	Блок параметров, в котором можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий. Тип преобразования можно выбрать в раскрывающемся списке. С помощью кнопок **Добавить преобразование** и **Удалить** можно добавить или удалить преобразование. Порядок преобразований имеет значение.

Возможность использовать преобразования зависит от типа используемого поля расширенной схемы событий:

- Для дополнительного поля с типом `Строка` доступны все типы преобразования.
- Для полей с типами `Число` и `Число с плавающей точкой` доступны типы преобразования **regexp**, **substring**, **replace**, **trim**, **append**, **prepend**, **replaceWithRegexp**, **decodeHexString**, **decodeBase64String** и **decodeBase64URLString**.
- Для полей с типами `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой` доступны типы преобразования **append** и **prepend**.

Посмотреть доступные преобразования

Преобразования – это изменения, которые применяются к значению перед записью в поле события.

Вы можете выбрать в раскрывающемся списке один из следующих типов преобразования:

- **entropy** – используется для преобразования значения исходного поля с помощью функции вычисления информационной энтропии и помещения результата преобразования в целевое поле типа `float`. Результатом преобразования будет число. Показатель вычисления информационной энтропии позволяет выявлять DNS-туннели и компрометацию паролей, например, когда пользователь ввел пароль вместо логина и пароль записывается в журнал в открытом виде.
- **lower** – используется для перевода всех символов значения в нижний регистр.
- **upper** – используется для перевода всех символов значения в верхний регистр.
- **regexp** – используется для преобразования значения с помощью указанного регулярного выражения RE2. При выборе этого типа преобразования отображается поле, в котором вам нужно указать регулярное выражение RE2.
- **substring** – используется для извлечения символов в указанном диапазоне позиций. При выборе этого типа преобразования отображаются поля **Начало** и **Конец**, в которых вам нужно указать диапазон позиций.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. При выборе этого типа преобразования отображаются следующие поля:
  - **Символы на замену** – последовательность символов, которую требуется заменить.
  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

- **trim** – используется для удаления указанных символов одновременно с начала и с конца значения поля события. При выборе этого типа преобразования отображается поле **Символы**, в котором вам нужно указать символы. Например, если для значения `Microsoft-Windows-Sysmon` требуется выполнить преобразование **trim** со значением `Micromon`, новым значением будет `soft-Windows-Sys`.

- **append** – используется для добавления указанных символов в конец значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **prepend** – используется для добавления указанных символов к началу значения поля события. При выборе этого типа преобразования отображается поле **Константа**, в котором вам нужно указать символы.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на указанную последовательность символов. При выборе этого типа преобразования отображаются следующие поля:

  - **Выражение** – регулярное выражение RE2, результаты которого требуется заменить.

  - **Чем заменить** – последовательность символов, которую требуется использовать вместо заменяемой последовательности символов.

- Конвертация закодированных строк в текст:

  - **decodeHexString** – используется для конвертации HEX-строки в текст.

  - **decodeBase64String** – используется для конвертации Base64-строки в текст.

  - **decodeBase64URLString** – используется для конвертации Base64url-строки в текст.

  - **unicodeUnescape** – используется для конвертации Unicode-строки в текст.

  При конвертации поврежденной строки или при ошибках конвертации в поле события могут быть записаны поврежденные данные.

  При обогащении событий, если длина закодированной строки превышает размер поля нормализованного события, строка будет обрезана и не будет раскодирована.

  Если длина раскодированной строки превышает размер поля события, в которое должно быть помещено раскодированное значение, строка будет обрезана до размера этого поля события.

  Мы не рекомендуем использовать несколько дополнительных нормализаторов для последовательного преобразования одного и того же поля. Результат одного преобразования, выполненного дополнительным нормализатором, не используется как входные данные для следующего. В итоговое событие записывается значение, полученное в дополнительном нормализаторе, который первым выполнил обогащение этого поля.

- Преобразование формата IP-адреса в IPv4:

  - **ipDecimalToDotted** – используется для преобразования IP-адреса в формате десятичного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.

  - **ipHexToDotted** – используется для преобразования IP-адреса в формате шестнадцатиричного числа в IP-адрес в формате IPv4, в котором октеты разделены точками.

- **hexToDecimal** – используется для преобразования числового значения, представленного в шестнадцатеричной системе счисления, в десятичный формат. Преобразование применяется к строковым или числовым полям, содержащим HEX-значения (включая префикс 0x, если он присутствует), и результат записывается в целевое поле события Kaspersky SIEM Cloud в виде целого числа.

  Результатом преобразования является число в десятичной системе, например исходное значение – 0x00FF, после преобразования – 255.

шаблон

Этот тип обогащения используется, если в поле события нужно записать значение, полученное при обработке шаблонов Go. Мы рекомендуем сопоставлять значение и размер поля. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "шаблон"

Параметр	Описание
Шаблон	Шаблон Go. Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт, например `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.
Целевое поле	Поле события, в которое требуется поместить данные.

Если вы используете обогащение событий, у которого в качестве параметра **Тип источника данных** выбрано значение **шаблон**, целевым полем является поле с типом `Строка`, а исходным полем является поле расширенной схемы событий, содержащее массив строк, то в шаблоне может быть использован один из следующих примеров:

- `{{.SA.StringArrayOne}}`
- ```
  {{- range $index, $element := . SA.StringArrayOne -}}
  {{- if $index}}, {{end}}"{{$element}}"{{- end -}}
  ```

Для преобразования в шаблоне данных поля массива в формат TSV требуется использовать функцию `toString`, например:

```
template {{toString .SA.StringArray}}
```

таблица

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря типа **Таблица**. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "таблица"

Параметр	Описание
Название словаря	Словарь, из которого будут браться значения.
Ключевые поля	Поля событий, значения которых будут использоваться для выбора записи словаря. Для добавления поля события нажмите на кнопку **Добавить поле**. Вы можете добавить несколько полей событий.
Сопоставление	Поля событий для передачи данных: • **Поле словаря** – поля словаря, из которых будут передаваться данные. Доступные поля зависят от выбранного ресурса словаря. • **Поле KUMA** – поля событий, в которые будут передаваться данные. Для выбранных полей (`*custom*` и `*flex*`) в столбце **Подпись** вы можете задать название для помещаемых данных.
```

Первое поле в таблице (**Поле словаря**) считается ключом, с которым будут сопоставляться поля, выбранные из события в качестве ключевых (**Поле KUMA**). В качестве ключа в **Поле словаря** вам нужно выбрать индикатор компрометации, по которому будет осуществляться обогащение, например IP-адрес, URL-адрес или хеш. В правиле необходимо выбрать поле события, соответствующее выбранному индикатору в поле словаря.

Если вы хотите выбрать несколько ключевых полей, вы можете указать их через разделитель `|` (при указании через веб-интерфейс или импорте через CSV-файл), например `<IP-адрес>|<имя пользователя>`.

Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить**. Для удаления строки таблицы нажмите на крестик ✕.

обогащение активами

Этот тип обогащения используется, когда необходимо добавить обогащение событий активами на определенных коллекторах.

Для обогащения событий активами в блоке **Сопоставление** требуется заполнить таблицу сопоставления полей события Kaspersky SIEM Cloud и полей для записи значениий из хеш-таблицы.

Чтобы заполнить таблицу сопоставления полей:

1. В блоке **Сопоставление** нажмите на кнопку **Добавить**.

2. В раскрывающемся списке **Поле KUMA** выберите одно или несколько полей события, значение которого будет сопоставляться со значением из хеш-таблицы и записываться в соответствующее поле в таблице данных актива.

3. В раскрывающемся списке **Поле для записи данных** выберите поле, в которое при соответствии поля события (**Поле KUMA**) и значения из хеш-таблицы будет записано значение идентификатора актива.

   Возможные значения параметров в таблице сопоставления полей

Поле KUMA	Поле для записи данных
DestinationAddress DestinationHostName DeviceAddress DeviceHostName SourceAddress SourceHostName DestinationMacAddress DeviceMacAddress SourceMacAddress DeviceCustomString1 DeviceCustomString2 DeviceCustomString3 DeviceCustomString4 DeviceCustomString5 DeviceCustomString6	SourceAssetID DeviceAssetID DestinationAssetID

   Если вы указываете несколько полей, к значениям полей применяется условие **И**. Если вы добавляете несколько строк в столбце **Поле KUMA**, к значениям полей применяется условие **ИЛИ**. Проверка начинается с первого поля в списке. Если значение поля совпадает со значением атрибута, проверка прекращается.

   Например, в событие поступают следующие данные:

   `SourceAddress=192.168.x.xx`
   `SourceHostName=kuma.example.com`

В Kaspersky SIEM Cloud есть два актива: `company.example.com` (IP-адрес: `192.168.x.xx`; FQDN: `company.example.com`) и `kuma.example.com` (IP-адрес: `192.168.y.yyy`; FQDN: `kuma.example.com`). Сопоставление для них осуществляется следующим образом:

- Если вы указали отдельно `sourceAddress` → `sourceAssetID`, а затем `sourceHostname` → `sourceAssetID`, то актив будет соответствовать первому условию (`company.example.com`).
- Если вам важнее получить значение параметра `sourceHostname` (`kuma.example.com`), то первым указывается `sourceHostname` → `sourceAssetID`, а затем `sourceAddress` → `sourceAssetID`.
- Если вы указали `sourceAddress` + `sourceHostname` → `sourceAssetID`, обогащение не произойдет.

> В таблице сопоставления полей требуется указать хотя бы одно условие сопоставления.

4. Если вы хотите применить для параметров **Поле KUMA** и **Поле для записи данных** значения по умолчанию, нажмите на кнопку. **Применить сопоставление по умолчанию**, расположенную над таблицей.

Значения параметров по умолчанию

Поле KUMA	Поле для записи данных
`DestinationAddress`	`DestinationAssetID`
`DestinationHostName`	`DestinationAssetID`
`DeviceAddress`	`DeviceAssetID`
`DeviceHostName`	`DeviceAssetID`
`SourceAddress`	`SourceAssetID`
`SourceHostName`	`SourceAssetID`

dns

Этот тип обогащения используется для отправки запросов на DNS-сервер частной сети для преобразования IP-адресов в доменные имена или наоборот. Преобразование IP-адресов в DNS-имена происходит только для частных адресов: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10, fd00::/8.

Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "dns"

Параметр	Описание
URL	URL DNS-сервера, которому вы хотите отправлять запросы. С помощью кнопки **Добавить URL** можно указать несколько URL. Если параметр **URL** не указан, то Kaspersky SIEM Cloud возьмет список DNS-серверов из файла `/etc/resolv.conf`, расположенного на локальном хосте. В этом случае вам нужно включить параметр **Требуется рекурсия**. В противном случае обогащение происходить не будет.
Запросов в секунду	Максимальное количество запросов к DNS-серверу в секунду. Значение по умолчанию: количество vCPU сервера, на котором установлено Ядро Kaspersky SIEM Cloud.
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Укажите целое положительное число от 0 до 999. Если указано 0, то используется число логических ядер CPU. Значение по умолчанию: `1`.
Максимальное число событий в очереди обогащения	Максимальное число событий, сохраняемое в очереди для повторной отправки. Значение по умолчанию: `1 000 000`.
Время ожидания	Время ожидания ответа от DNS-сервера (в секундах). Значение по умолчанию: `5`.

Параметр	Описание
Переопределение режима DNS	Используемый метод преобразования: • **Только прямое разрешение DNS** – доменное имя преобразуется в IP-адрес. • **Только обратное разрешение DNS** – IP-адрес преобразуется в доменное имя. • **Прямое и обратное DNS-разрешение** – доменное имя может преобразовываться в IP-адрес и наоборот.
Срок жизни кеша	Время жизни значений (в секундах), хранящихся в кеше. Значение по умолчанию: `60` (сек).
Кеш отключен	Параметр, позволяющий включить или выключить кеширование. По умолчанию кеширование включено.
Обновление кэша отключено	Если обновление кеша включено, то по истечении срока жизни кеша коллектор отправляет повторные запросы на DNS-сервер для обновления хранящихся в кеше данных. Этот параметр доступен только при включенном кеше. По умолчанию обновление кеша включено.
Требуется рекурсия	Параметр позволяет включить отправку коллектором рекурсивных запросов к авторитативным DNS-серверам для выполнения обогащения. Значение по умолчанию: **Выключено**.

cybertrace

Для систем с большой нагрузкой на коллектор или коррелятор рекомендуется использовать тип обогащения **cybertrace-http**. Этот тип обогащения возвращает структурированный ответ в формате JSON и корректно различает строки и массивы пользовательских атрибутов, исключая ошибки парсинга.
При обогащении с помощью типа **cybertrace** коллектор получает неструктурированный ответ. Если значение пользовательского атрибута в Kaspersky CyberTrace содержит квадратные скобки, например **[str1**, **str2]**, Kaspersky SIEM Cloud обрабатывает его как массив, а не как строку.

Этот тип обогащения используется для добавления в поля события сведений из потоков данных Kaspersky CyberTrace. Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "cybertrace"

Параметр	Описание
URL	URL сервера Kaspersky CyberTrace, которому вы хотите отправлять запросы. Порт Kaspersky CyberTrace по умолчанию: 9999. Обязательный параметр.
Количество подключений	Максимальное количество подключений к серверу Kaspersky CyberTrace, которые может одновременно установить Kaspersky SIEM Cloud. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро Kaspersky SIEM Cloud.
Запросов в секунду	Максимальное количество запросов к серверу в секунду. Значение по умолчанию: `1000`.
Время ожидания	Время ожидания отклика от сервера Kaspersky CyberTrace в секундах. Значение по умолчанию: `30`.
Максимальное кол-во событий в очереди обогащения	Максимальное количество событий, сохраняемое в очереди для переотправки. Значение по умолчанию: `1 000 000`.
Сопоставление	Таблица сопоставления полей событий с типами индикаторов Kaspersky CyberTrace. В столбце **Поле KUMA** указаны названия полей событий, а в столбце **Индикатор CyberTrace** указаны типы индикаторов Kaspersky CyberTrace. Доступные типы индикаторов Kaspersky CyberTrace: • **ip** • **url** • **hash**

В таблице сопоставления требуется указать как минимум одну строку. Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить строку**. Для удаления строки таблицы нажмите на крестик ✕.

cybertrace-http

Этот тип потокового обогащения событий в Kaspersky CyberTrace, который позволяет отправлять большое количество событий одним запросом на API-интерфейс CyberTrace. Мы рекомендуем применять тип обогащения **cybertrace-http** в системах с большим потоком событий. Производительность **cybertrace-http** превосходит показатели типа обогащения **cybertrace**.

Ограничения:

- Тип обогащения **cybertrace-http** невозможно использовать для ретроспективного сканирования в KUMA.
- В случае использования типа обогащения **cybertrace-http** обнаружения киберугроз не сохраняются в истории Kaspersky CyberTrace в окне **Обнаружения**.

Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "cybertrace-http"

Параметр	Описание
Тенант	Тенант, в рамках которого вы планируете работать с Kaspersky CyberTrace. Обязательный параметр.
URL	URL сервера Kaspersky CyberTrace, которому вы хотите отправлять запросы и порт, который использует API CyberTrace. Порт по умолчанию 443. Обязательный параметр.
Секрет	Раскрывающийся список для выбора секрета, в котором хранятся учетные данные для подключения. Обязательный параметр.
Время ожидания	Время ожидания отклика от сервера Kaspersky CyberTrace в секундах. Значение по умолчанию: `30`.
Ключевые поля	Список полей событий, используемых для обогащения событий данными из Kaspersky CyberTrace. Обязательный параметр.
Максимальное кол-во событий в очереди обогащения	Максимальное количество событий, сохраняемое в очереди для переотправки. Значение по умолчанию: `1 000 000`. По достижении 1 млн получаемых событий от сервера Kaspersky CyberTrace события перестают обогащаться, пока число получаемых событий не станет меньше 500 тыс.
Основная версия CyberTrace	Версия Kaspersky CyberTrace. Доступные значения: • **<5** – запросы будут выполняться в тенанте General в Kaspersky CyberTrace и будут использовать новую версию API, соответствующую Kaspersky CyberTrace 5.0 и выше. • **≥ 5.0** – запросы будут использовать версию API, соответствующую Kaspersky CyberTrace 4.x. Значение по умолчанию: **<5**.
Отладка	Параметр, включающий логирование ресурса. По умолчанию переключатель выключен.
Теги	Теги для поиска ресурса.

часовой пояс

Этот тип обогащения используется в коллекторах и корреляторах, чтобы присвоить событию определенный часовой пояс. Сведения о часовом поясе могут понадобиться при поиске событий, случившихся в нетипичное время, например ночью.

При выборе этого типа обогащения в раскрывающемся списке **Часовой пояс** нужно указать временную зону.

Убедитесь, что выбираемый часовой пояс установлен на сервере сервиса, использующего обогащение. Например, это можно сделать с помощью команды `timedatectl list-timezones`, которая показывает все установленные на сервере часовые пояса. Подробнее об установке часовых поясов смотрите в документации используемой вами операционной системы.

При обогащении события в поле события DeviceTimeZone записывается смещение времени выбранного часового пояса относительно всемирного координированного времени (UTC) в формате `+-чч:мм`. Например, если выбрать временную зону **Asia/Yekaterinburg** в поле `DeviceTimeZone` будет записано значение `+05:00`. Если в обогащаемом событии есть значение поля `DeviceTimeZone`, оно будет перезаписано.

По умолчанию, если в обрабатываемом событии не указан часовой пояс и не настроены правила обогащения по часовому поясу, событию присваивается часовой пояс сервера, на котором установлен сервис (коллектор или коррелятор), обрабатывающий событие. При изменении времени сервера сервис требуется перезапустить.

Допустимые форматы времени при обогащении поля DeviceTimeZone

При обработке в коллекторе поступающих сырых событий следующие форматы времени могут быть автоматически приведены к формату `+-чч:мм` (см. таблицу ниже):

Формат времени в обрабатываемом событии	Пример
+-чч:мм	-07:00
+-ччмм	-0700
+-чч	-07

Если формат даты в поле `DeviceTimeZone` отличается от указанных в таблице, при обогащении события сведениями о часовом поясе в поле записывается часовой пояс серверного времени коллектора. Вы можете создать правила нормализации для нестандартных форматов времени.

геоданные

Этот тип обогащения используется для добавления в поля событий сведений о географическом расположении IP-адресов.

При выборе этого типа в блоке параметров **Сопоставление геоданных с полями события** укажите, из какого поля события будет считан IP-адрес, а также выберите атрибуты геоданных и определите поля событий, в которые геоданные будут записаны:

1. В раскрывающемся списке **Поле события с IP-адресом** выберите поле события, из которого считывается IP-адрес. По этому IP-адресу будет произведен поиск соответствий по загруженным в Kaspersky SIEM Cloud геоданным.

   > При выборе полей события `SourceAddress`, `DestinationAddress` и `DeviceAddress` становится доступна кнопка **Применить сопоставление по умолчанию**. С ее помощью можно добавить преднастроенные пары соответствий атрибутов геоданных и полей события.

2. Для каждого поля события, откуда требуется считать IP-адрес, выберите тип геоданных и поле события, в которое следует записать геоданные.

   - В поле **Атрибут геоданных** выберите, какие географические сведения, соответствующие считанному IP-адресу, необходимо записать в событие. Доступные атрибуты геоданных: **Страна**, **Регион**, **Город**, **Долгота**, **Широта**.

   - В поле **Поле события для записи** выберите поле события, в которое необходимо записать выбранный атрибут геоданных.

   С помощью кнопки **Добавить атрибут геоданных** вы можете добавить пары полей **Атрибут геоданных – Поле события для записи**. Так вы можете настроить запись разных типов геоданных одного IP-адреса в разные поля события.

3. Для добавления каждого последующего сопоставления используйте кнопку **Добавить сопоставление** и повторяйте предыдущие два пункта инструкции.

   Вы можете записать одинаковые атрибуты геоданных в разные поля событий. Если вы настроите запись нескольких атрибутов геоданных в одно поле события, событие будет обогащено последним по очереди сопоставлением.

проверка DLL Hijacking

DLL Hijacking – это техника атаки, которая заключается в том, что на целевую систему доставляется уязвимое легитимное программное обеспечение вместе с вредоносной динамической библиотекой (DLL). Для обнаружения таких атак Kaspersky SIEM Cloud использует модуль AI. Модуль AI анализирует параметры запуска и исполнения программ и определяет подозрительные случаи запуска легитимного программного обеспечения с вредоносными библиотеками.

Для получения заключения Kaspersky SIEM Cloud отправляет запрос с информацией из полей события в <KSN>. В ответ на запрос KSN присылает результат анализа.

Вы можете настроить обнаружение атак DLL Hijacking в коллекторе или коррелляторе.

Для использования обогащения типа **Проверка DLL Hijacking** ваша лицензия должна включать в себя модуль AI. Главному администратору также требуется принять дополнительное Положение о KSN в блоке **Kaspersky Security Network** (**Параметры → KUMA → Открыть параметры KUMA → Интеграции → AI-сервисы → Обнаружение атак DLL Hijacking**).

Параметры этого типа обогащения описаны в таблице ниже.

Параметры типа обогащения "DLL Hijacking"

Параметр	Описание
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки событий. Укажите целое положительное число от 0 до 999. Если указано 0, то используется число логических ядер CPU.
Максимальный размер кеша	Максимальный размер кеша для ответов, получаемых из KSN, в мегабайтах. Значение по умолчанию: `128 МБ`. Каждый ответ из KSN имеет свое время жизни, в течение которого он хранится в кеше. Если Kaspersky SIEM Cloud отправляет повторный запрос по файлу DLL, для которого KSN уже выдал ответ, и время жизни этого ответа еще не истекло, то запрос не отправляется в KSN, а ответ берется из кеша.
Максимальное количество событий в очереди обогащения	При превышении указанного значения, новые события обрабатываться не будут. Значение по умолчанию: `1 000 000`. Значение `0` означает, что при возникновении очереди события перестают обогащаться.

Выполнять повторный запрос	В ответе KSN может выдать заключение **В обработке**. Этот заключение означает, что KSN принял запрос и в данный момент обрабатывает его, но заключения пока нет. Обработка может занять длительное время, поэтому требуется повторная отправка запроса.
	Если этот параметр включен, настройте дополнительные параметры:
	• **Создавать дубликаты событий** – если этот параметр включен, Kaspersky SIEM Cloud создает дубликат события и использует его для повторных запросов к KSN. Основное событие при этом отправляется дальше по потоку. Дубликат события будет записан в базу данных, когда выполнится одно из следующих условий:
	  • Из KSN получено заключение, отличное от **В обработке**.
	  • Переполнен дисковый буфер, размер которого указан в параметре **Размер буфера**.
	  • Превышено значение, указанное в параметре **Количество запросов**.
	  Если этот параметр выключен, Kaspersky SIEM Cloud продолжит отправлять запросы с использованием основного события. Событие будет записано в базу данных, когда выполнится одно из следующих условий:
	  • Из KSN получено заключение, отличное от **В обработке**.
	  • Переполнен дисковый буфер, размер которого указан в параметре **Размер буфера**.
	  • Превышено значение, указанное в параметре **Количество запросов**.
	• **Количество запросов** – максимальное количество запросов в KSN. Если за указанное количество запросов так и не будет получено заключение, отличное от **В обработке**, событие будет записано в базу данных с заключением **В обработке**. Значение по умолчанию: `10`.
	• **Интервал запросов** – интервал между запросами, в минутах. Значение по умолчанию: `1 минута`. Минимальное значение: `1 минута`.
	• **Размер буфера** – размер дискового буфера, который используется для хранения событий, ожидающих повторного запроса, в мегабайтах. Значение по умолчанию: `10240 МБ`. Минимальное значение: `10 МБ`.

Прокси-сервер	Параметры прокси-сервера, если он требуется для подключения к серверу KSN. Можно выбрать один из доступных или создать новый прокси-сервер. По умолчанию прокси-сервер не используется.
Сопоставление	Таблица параметров, которые нужно отправить в запросе в KSN для получения заключения, и соответствующих полей событий Kaspersky SIEM Cloud: • **Хеш файла DLL (md5)** – рекомендованное поле для сопоставления: `OldFileHash`. • **Путь до файла DLL** – полный путь, включающий имя файла. Рекомендованное поле для сопоставления: `OldFilePath`. Так как путь может содержать персональные данные, Kaspersky SIEM Cloud передает этот параметр в KSN в обезличенном виде. Например: Путь до обезличивания: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll` Тот же путь в обезличенном виде: `device\harddiskvolume1\users\username` • **Хеш процесса (md5)** – рекомендованное поле для сопоставления: `FileHash`. • **Путь до процесса** – полный путь, включающий имя файла. Так как путь может содержать персональные данные, Kaspersky SIEM Cloud передает этот параметр в KSN в обезличенном виде. Например: Путь до обезличивания: `C:\Windows\Device\HarddiskVolume1\Users\Alex\malware.dll` Тот же путь в обезличенном виде: `device\harddiskvolume1\users\username` • **Имя файла DLL** – рекомендованное поле для сопоставления: `OldFileName`. • **Имя процесса** – рекомендованное поле для сопоставления: `FileName`. • **Подпись процесса** – поле, в котором указывается поле Kaspersky SIEM Cloud, которое передает `Organization` из `Subject` подписи. Если этих значений нет, подпись стоит оставить пустой. Чтобы добавить этот параметр, нажмите на кнопку **Добавить**, затем в столбце **Поле DLL Hijacking** в выпадающем списке выберите **подпись процесса**.необязательный параметр. Рекомендованное поле для сопоставления: FileID. • **Размер файла DLL** – необязательный параметр; рекомендованное поле для сопоставления: OldFileSize. Чтобы добавить этот параметр, нажмите на кнопку **Добавить**, затем в столбце **Поле DLL Hijacking** в выпадающем списке выберите **размер файла DLL**. Для каждого параметра укажите в таблице соответствующее ему поле события Kaspersky SIEM Cloud.

5. Если требуется включить логирование операций сервиса, включите переключатель **Отладка**.

6. При необходимости в раскрывающемся списке **Теги** выберите теги для правила обогащения.

7. При необходимости в поле **Описание** добавьте описание правила обогащения. Описание правила может содержать до 4000 символов в кодировке Unicode.

8. Если вы хотите задать условия определения событий, которые будут обрабатываться с применением правила обогащения, в блоке **Параметры фильтра** в раскрывающемся списке **Фильтр** выберите или создайте фильтр.

   Как создать фильтр

Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

Чтобы создать фильтр:

1. В раскрывающемся списке **Фильтр** выберите **Создать**.
2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят.
3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.
4. Выберите режим создания фильтра: **Конструктор** или **Код**.

   При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра.
5. Если вы выбрали вариант **Конструктор**, выполните следующие действия:

   a. В раскрывающемся списке выберите логический оператор:

   - **И** – отбирает события, которые соответствуют всем указанным условиям.
   - **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий.
   - **НЕ** – отбирает события, которые не соответствуют всем указанным условиям.

   b. Нажмите на кнопку **Добавить условие**.

   c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

   d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра.

   Операнды фильтров

   - **Поля событий** – поле события, которое требуется использовать как операнд фильтра.
   - **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**.

     Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра.

- **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры:
  - **словарь** (обязательно) – словарь, который требуется использовать.
  - **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.
- **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события.
  - **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать.
  - **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы.
  - **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда.
  - **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда.
- **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
  - **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**.
  - **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.
- **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
  - **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
  - **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
  - **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.
- **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
  - **значение** (обязательно) – константа, которую требуется присвоить операнду.
- **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
  - **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.

Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в коррелляторах.

- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.

Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.

e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.

Вы можете добавить несколько групп условий.

6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.

В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка . Если вы хотите удалить условие, нажмите на значок удаления .

8. Нажмите **Сохранить**.

9. Нажмите на кнопку **Создать**.

Правило обогащения будет создано и отобразится в таблице.

Привязка правил обогащения

Чтобы привязать правило обогащения к коллектору и/или коррелятору:

1. В веб-интерфейсе откройте раздел **Мониторинг → Ресурсы и сервисы → Правила обогащения**.

Отобразится таблица правил обогащения.

2. Установите флажок рядом с одним или несколькими правилами обогащения.

3. В панели инструментов или в меню нажмите **Привязать к сервису** и выберите один из следующих вариантов:

- **Привязать к коллектору**.
- **Привязать к коррелятору**.

4. В открывшейся панели выберите один или несколько коррелляторов или коллекторов и нажмите **ОК**.

Правило обогащения будет привязано к выбранным сервисам и начнет выполняться в соответствии с их конфигурацией.

Вы можете отвязать правило обогащения от коллектора и/или коррелятора при изменении правила.

Управление правилами обогащения

В этой статье описано, как изменить и дублировать правило обогащения, как просмотреть зависимости и версии, а также как удалить правило.

Изменение правила обогащения

Чтобы изменить правило обогащения:

1. В веб-интерфейсе откройте один из следующих разделов:

   - **Мониторинг → Ресурсы и сервисы → Правила обогащения**.
   - **Мониторинг → Ресурсы и сервисы → Список**.

     При выборе этого раздела для удобства отображения объектов в столбце **Тип ресурса** выберите **Правило обогащения**.

2. Нажмите на правило обогащения, которое вы хотите изменить.

   Справа откроется панель **Редактирование правила обогащения**.

3. Внесите необходимые изменения.

4. Если вы хотите привязать правило обогащения к коллектору или коррелятору либо отвязать правило, откройте вкладку **Сервисы** и выполните следующие действия:

   - Для того чтобы привязать правило обогащения, нажмите **Привязать к сервису** и выберите **Привязать к коллектору** или **Привязать к коррелятору**. В открывшейся панели выберите один или несколько коллекторов и/или корреляторов и нажмите **ОК**.
   - Для того чтобы отвязать правило обогащения, установите флажки рядом с нужными коллекторами и/или корреляторами, нажмите **Удалить** и подтвердите удаление.

5. Нажмите **Сохранить**.

Правило обогащения будет изменено.

Создание правила обогащения на основе существующего

Чтобы создать копию правила обогащения:

1. В веб-интерфейсе откройте один из следующих разделов:

   - **Мониторинг → Ресурсы и сервисы → Правила обогащения**.
   - **Мониторинг → Ресурсы и сервисы → Список**.

     При выборе этого раздела для удобства отображения объектов в столбце **Тип ресурса** выберите **Правило обогащения**.

2. Установите флажок рядом с правилом обогащения, которое вы хотите копировать.
3. В панели инструментов или в меню ⋮ нажмите **Дублировать**.
4. В открывшейся панели **Создание правила обогащения** укажите параметры создаваемого правила.
5. Нажмите **Сохранить**.

Правило обогащения будет создано на основе существующего правила.

Просмотр зависимостей

Для каждого правила обогащения вы можете открыть граф зависимостей.

Чтобы просмотреть зависимости:

1. В веб-интерфейсе откройте один из следующих разделов:
   - **Мониторинг → Ресурсы и сервисы → Правила обогащения**.
   - **Мониторинг → Ресурсы и сервисы → Список**.

     При выборе этого раздела для удобства отображения объектов в столбце **Тип ресурса** выберите **Правило обогащения**.
2. Установите флажок рядом с нужным правилом обогащения.
3. В панели инструментов или в меню ⋮ нажмите **Показать зависимости**.

   Откроется окно зависимостей правила обогащения.
4. Если вы хотите скачать данные о зависимостях, нажмите на кнопку **Скачать в формате SVG**.
5. Если требуется, настройте фильтры для отображения зависимостей на графе с помощью раскрывающегося списка **Показывать на графе**.

Просмотр истории версий

Чтобы просмотреть историю версий правила обогащения:

1. В веб-интерфейсе откройте один из следующих разделов:
   - **Мониторинг → Ресурсы и сервисы → Правила обогащения**.
   - **Мониторинг → Ресурсы и сервисы → Список**.

     При выборе этого раздела для удобства отображения объектов в столбце **Тип ресурса** выберите **Правило обогащения**.
2. Установите флажок рядом с правилом обогащения, версии которого вы хотите просмотреть.
3. В панели инструментов или в меню ⋮ нажмите **Показать историю версий**.

4. При необходимости вы можете сравнить версии между собой. Для этого установите флажки рядом с версиями, которые вы хотите сравнить, и нажмите **Сравнить**.

5. Если вы хотите восстановить более раннюю версию правила, установите флажок рядом с названием этого правила, нажмите **Восстановить** и затем подтвердите восстановление.

Удаление правила обогащения

Чтобы удалить правило обогащения:

1. В веб-интерфейсе откройте один из следующих разделов:

   - **Мониторинг → Ресурсы и сервисы → Правила обогащения**.
   - **Мониторинг → Ресурсы и сервисы → Список**.

     При выборе этого раздела для удобства отображения объектов в столбце **Тип ресурса** выберите **Правило обогащения**.

2. Установите флажки рядом с правилами обогащений, которые вы хотите удалить.

3. В панели инструментов или в меню ⋮ нажмите **Удалить**.

4. Подтвердите удаление.

Правила обогащения будут удалены.

Добавление правил обогащения в свойствах коллектора

Вы можете настроить обогащение событий, поступающих только на те коллекторы, для которых это необходимо. Для этого добавьте одно или несколько правил обогащения в свойствах коллектора.

Чтобы добавить правила обогащения в свойствах коллектора:

1. В веб-интерфейсе откройте раздел **Мониторинг → Ресурсы и сервисы → Коллекторы** и выберите нужный тенант.

   Откроется таблица коллекторов.

2. Нажмите на название коллектора, для которого вы хотите добавить правило обогащения.

3. В открывшейся боковой панели выберите раздел **Обогащение событий**.

4. Нажмите на кнопку **Добавить обогащение**.

5. В раскрывающемся списке **Правило обогащения** выберите правило обогащения.

   Вы также можете создать правило обогащения коллектора, нажав **Создать** в раскрывающемся списке **Правило обогащения**.

6. При необходимости добавьте другое правило обогащения, нажав на кнопку **Добавить обогащение**.

> Добавить одно и тоже правило обогащения повторно невозможно.

7. Нажмите **Сохранить**.

Добавленное правило обогащения будет применяться Kaspersky SIEM при получении и обработке коллектором сообщений из источников событий.

Обогащение событий активами

К корпоративной сети компании может быть подключено множество устройств (активов) различных типов, например серверы, рабочие станции, ноутбуки, мобильные устройства, IoT-устройства. Активы идентифицируются по таким свойствам как IP-адрес, FQDN, MAC-адрес. Для обеспечения безопасности корпоративной сети вам может понадобиться:

- отслеживать активы и их свойства при корреляции и для проведения расследований;
- использовать активы и их свойства для срабатывания правил корреляции;
- отслеживать состояние активов на виджетах и в отчетах;
- иметь актуальный список активов с незакрытыми уязвимостями;
- контролировать трафик с IoT-устройств, например с веб-камер, холодильников, кофе-машин.

Для решения этих задач можно использовать обогащение событий активами.

Настройка обогащения событий активами состоит из следующих этапов:

1. **Добавление активов в Kaspersky SIEM Cloud и заполнение их свойств**

   Это можно сделать следующими способами:

   - Импортировать активы из:
     - Kaspersky Security Center Windows или Kaspersky Security Center Linux;
     - KICS for Networks или KATA;
     - MaxPatrol VM;
     - отчета nmap.
   - Добавить активы вручную.
   - Добавить активы по REST API.

2 Добавление настраиваемых полей в свойства активов

Если вам недостаточно существующих полей модели данных актива, вы можете создать настраиваемые поля активов и затем добавить в эти поля значения в свойствах активов вручную или через REST API.

Например, если вы хотите разделять IoT-устройства по типам, вы можете создать настраиваемое поле `IoT type`. Затем вам нужно найти в разделе **Активы** веб-интерфейса Kaspersky SIEM Cloud все IoT-устройства и в свойствах каждого устройства указать тип устройства в поле `IoT type`, например: `webcam`, `refrigerator`, `coffee machine`.

3 Настройка категоризации активов

Вы можете сгруппировать активы в категории, которые можно использовать при настройке правил корреляции. При создании категорий вы можете использовать свойства активов в качестве условий наполнения категорий, например наличие уязвимостей, тип IoT-устройства или актуальность антивирусных баз. Каждой категории вы можете назначить уровень важности от низкого до критического.

4 Настройка правил обогащения событий активами

Так как обогащение активами повышает нагрузку на сервис коллектора, рекомендуется выбрать, на каких коллекторах вы хотите настроить обогащение активами. Это можно сделать исходя из типа и функции источников событий, которые отправляют события в коллектор. Вы можете настроить обогащение активами на всех коллекторах и позднее выключить обогащение на тех коллекторах, для которых оно не требуется.

Обогащение событий активами настраивается на шаге **Обогащение событий** при создании коллектора. Для этого вам нужно создать и настроить правило обогащения с типом **обогащение активами**. Вы можете это сделать либо на шаге **Обогащение событий**, либо создать правило обогащения предварительно и затем привязать его в коллекторе.

Логика работы правила обогащения активами следующая. Когда в коллектор поступает событие, Kaspersky SIEM Cloud проверяет, заполнены ли поля `SourceAddress`, `DestinationAddress`, `DeviceAddress`, `SourceHostName`, `DestinationHostName` и `DeviceHostName`. Значения IP-адреса или FQDN из этих полей затем сверяются со значениями IP-адресов и FQDN из свойств активов, добавленных в Kaspersky SIEM Cloud. Таким образом, совпадение значений из полей события и из свойств актива позволяет определить, какой именно актив указан в событии. Далее Kaspersky SIEM Cloud прописывает значение `AssetID` найденного актива в одно или несколько из следующих полей события: `SourceAssetID`, `DestinationAssetID`, `DeviceAssetID`. После этого события направляются в коррелятор или хранилище.

Например, в событие поступают следующие данные:

`SourceAddress=192.168.x.xx`
`SourceHostName=kuma.example.com`

В Kaspersky SIEM Cloud есть два актива: `company.example.com` (IP-адрес: `192.168.x.xx`; FQDN: `company.example.com`) и `kuma.example.com` (IP-адрес: `192.168.y.yyy`; FQDN: `kuma.example.com`). Сопоставление для них осуществляется следующим образом:

- Если вы указали отдельно `sourceAddress` → `sourceAssetID`, а затем `sourceHostname` → `sourceAssetID`, то актив будет соответствовать первому условию (`company.example.com`).
- Если вам важнее получить значение параметра `sourceHostname` (`kuma.example.com`), то первым указывается `sourceHostname` → `sourceAssetID`, а затем `sourceAddress` → `sourceAssetID`.
- Если вы указали `sourceAddress` + `sourceHostname` → `sourceAssetID`, обогащение не произойдет.

Возможные значения параметров в таблице сопоставления полей

Поле KUMA	Поле для записи данных

`DestinationAddress`
`DestinationHostName`
`DeviceAddress`
`DeviceHostName`
`SourceAddress`
`SourceHostName`
`DestinationMacAddress`
`DeviceMacAddress`
`SourceMacAddress`
`DeviceCustomString1`
`DeviceCustomString2`
`DeviceCustomString3`
`DeviceCustomString4`
`DeviceCustomString5`
`DeviceCustomString6`
	`SourceAssetID`
	`DeviceAssetID`
	`DestinationAssetID`

Выполнение этого сценария позволит вам следующее:

- При работе с событиями вы сможете открыть свойства актива и посмотреть детальную информацию, например, об уязвимостях актива и состоянии его антивирусной защиты.
- В поисковых запросах, в виджетах и отчетах вы сможете использовать функции enrich_assets и lookup_assets.
- Вы сможете использовать в селекторах правил корреляции условия типа `inCategory`, что позволит учитывать в корреляционной логике произвольные свойства активов, например отслеживать интернет-трафик для категории IoT-устройств, таких как веб-камеры, кофе-машины или холодильники.
- Алертам будет присваиваться уровень важности на основании уровня важности категорий активов. Например, если в алерте присутствует актив с категорией Vulnerable, то у алерта будет высокий уровень важности.
- Вы сможете создавать и выгружать в файл CSV список активов, удовлетворяющих поисковому фильтру, например список кофе-машин с незакрытой уязвимостью.

Обогащение событий геоданными

Некоторые события, поступающие в Kaspersky SIEM Cloud, содержат белые (публичные) IP-адреса. Вам может понадобиться информация о том, каким геолокациям соответствуют белые IP-адреса в событиях. Для решения этой задачи вы можете использовать обогащение событий геоданными.

Чтобы настроить обогащение событий геоданными:

1. Сконвертируйте геоданные в формат Kaspersky SIEM Cloud.
2. Импортируйте сконвертированные геоданные в Kaspersky SIEM Cloud.
3. Создайте правило обогащения с типом **геоданные** одним из следующих способов:
   - В разделе **Обогащение событий** при создании коллектора.
   - Аналогично предыдущему способу в свойствах уже установленного коллектора в разделе **Обогащение событий**.
   - Отдельно как ресурс.

4. Если вы создали правило обогащения с типом **геоданные** отдельно как ресурс, добавьте его в свойствах коллекторов, обрабатывающих события с белыми IP-адресами.

5. Обновите конфигурации коллекторов, к которым вы добавили правило обогащения с типом геоданные.

Формат геоданных

Геоданные можно загрузить в Kaspersky SIEM Cloud в виде CSV-файла в кодировке UTF-8 (см. таблицу ниже). В качестве разделителя используется запятая. В первой строке файла указаны заголовки полей: `Network`, `Country`, `Region`, `City`, `Latitude`, `Longitude`.

Описание CSV-файла

Имя заголовка поля в CSV	Описание поля	Пример
`Network`	IP-адрес в одном из следующих форматов: • единичный IP-адрес; • диапазон IP-адресов; • IP-адрес в формате CIDR. Допускается перемешивание IPv4- и IPv6-адресов. Обязательное поле.	• `192.168.2.24` • `192.168.2.25-192.168.2.35` • `131.10.55.70/8` • `2001:DB8::0/120`
`Country`	Принятое в вашей организации обозначение страны, например название или код. Обязательное поле.	• `Russia` • `RU`
`Region`	Принятое в вашей организации обозначение области, например название или код.	• `Sverdlovsk Oblast` • `RU-SVE`
`City`	Принятое в вашей организации обозначение города, например название или код.	• `Yekaterinburg` • `65701000001`
`Latitude`	Широта описываемой точки в десятичном формате. Поле может быть пустым. В этом случае при импорте в Kaspersky SIEM Cloud будет использовано значение 0.	`56.835556`
`Longitude`	Долгота описываемой точки в десятичном формате. Поле может быть пустым. В этом случае при импорте в Kaspersky SIEM Cloud будет использовано значение 0.	`60.612778`

Конвертация геоданных из MaxMind и IP2Location

Если исходные файлы будут содержать другой набор полей, отличный от указанного в этом разделе, или каких-то полей будет не хватать, после конвертации отсутствующие поля в итоговом CSV-файле будут пустыми.

В Kaspersky SIEM Cloud можно использовать геоданные, полученные из MaxMind, IP2Location, а также совместимые с ними по формату. Перед использованием архивы с файлами геоданных в формате CSV требуется конвертировать в поддерживаемый решением формат. Наименование конвертируемых CSV-файлов внутри архивов должно соответствовать шаблонам:

- `(GeoIP2|GeoLite2|RU-GeoIP)-(City|Country)-Blocks-IPv(4|6).csv`
- `(GeoIP2|GeoLite2|RU-GeoIP)-(City|Country)-Locations-%s.csv`

CSV-файлы с геоданными не должны содержать дублирующихся записей. Например, если в файле мало столбцов, в разные записи могут попадать данные одной и той же сети с теми же геоданными и такой файл конвертировать не удастся. Для успешной конвертации нужно проверить, что дублирующиеся строки отсутствуют и все строки уникальны по какому-либо полю.

Конвертацию можно произвести с помощью скрипта, который можно скачать по ссылке:

Скачать скрипт

Для запуска скрипта требуется Python 2.7 или выше.

Команда запуска скрипта

```
python converter.py --type <geographic_data_type> --out <directory> --input <path>
```

где:

`<geographic_data_type>` – тип обрабатываемых геоданных: ("maxmind" или "ip2location");

`<directory>` – директория, в которую будет помещен CSV-файл с геоданными в формате Kaspersky SIEM Cloud;

`<path>` – путь к ZIP-архиву с геоданными из MaxMind или IP2location.

При запуске скрипта с флагом `--help` отображается справка по доступным параметрам запуска скрипта:

```
python converter.py --help
```

Команда для конвертации файла с российской базой диапазонов IP-адресов из ZIP-архива MaxMind

```
python converter.py --type maxmind --lang ru --input MaxMind.zip --out geoip_maxmind_ru.csv
```

Без указания параметра `--lang` скрипт по умолчанию получает информацию из файла `GeoLite2-City-Locations-en.csv` из ZIP-архива. Отсутствие параметра `--lang` для MaxMind равнозначно команде:

```
python converter.py --type maxmind --input MaxMind.zip --out geoip_maxmind.csv
```

Команда для конвертации файла из ZIP-архива IP2Location

```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP --out geoip_ip2location.csv
```

Команда для конвертации файла из нескольких ZIP-архивов IP2Location

```
python converter.py --type ip2location --input IP2LOCATION-LITE-DB11.CSV.ZIP IP2LOCATION-LITE-DB11.IPV6.CSV.ZIP --
out geoip_ip2location_ipv4_ipv6.csv
```

Параметр `--lang` для IP2Location не используется.

Обязательные наборы полей

Исходные файлы MaxMind `GeoLite2-City-Blocks-IPv4.csv` и `GeoLite2-City-Blocks-IPv6.csv` должны содержать следующий набор полей: `network`, `geoname_id`, `registered_country_geoname_id`, `represented_country_geoname_id`, `is_anonymous_proxy`, `is_satellite_provider`, `postal_code`, `latitude`, `longitude`, `accuracy_radius`

Пример набора исходных данных

```
network,geoname_id,registered_country_geoname_id,represented_country_geoname_id,
is_anonymous_proxy,is_satellite_provider,postal_code,latitude,longitude,accuracy_radius
1.0.0.0/24,2077456,2077456,,0,0,,-33.4940,143.2104,1000
1.0.1.0/24,1814991,1814991,,0,0,,34.7732,113.7220,1000
```

Остальные CSV-файлы с кодом локализации должны содержать следующий набор полей: `geoname_id`, `locale_code`, `continent_code`, `continent_name`, `country_iso_code`, `country_name`, `subdivision_1_iso_code`, `subdivision_1_name`, `subdivision_2_iso_code`, `subdivision_2_name`, `city_name`, `metro_code`, `time_zone`, `is_in_european_union`

Пример набора исходных данных

```
geoname_id,locale_code,continent_code,continent_name,country_iso_code,country_name,subdivision_1_iso_code,subdivision
1392,de,AS,Asien,IR,Iran,02,Mazandaran,,,,,Asia/Tehran,0
7240,de,AS,Asien,IR,Iran,28,Nord-Chorasan,,,,,Asia/Tehran,0
```

Исходные файлы IP2Location должны содержать данные о диапазонах сетей: `Country`, `Region`, `City`, `Latitude`, `Longitude`.

Пример набора исходных данных

```
"0","16777215","-","-","-","-","0.000000","0.000000","-","-"
"16777216","16777471","US","United States of America","California","Los
Angeles","34.052230","-118.243680","90001","-07:00"
"16777472","16778239","CN","China","Fujian","Fuzhou","26.061390","119.306110","350004","+08:00"
```

Импорт и экспорт геоданных

Вы можете вручную импортировать и экспортировать геоданные. Геоданные импортируются и экспортируются в CSV-файл. При успешном импорте геоданных ранее добавленные данные перезаписываются и в Kaspersky SIEM Cloud создается событие аудита.

Чтобы импортировать геоданные:

1. Подготовьте CSV-файл с геоданными.

   Геоданные, полученные из MaxMind и IP2Location, требуется конвертировать в поддерживаемый формат.

2. В веб-консоли откройте раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

3. В блоке **Другое** нажмите **Общие**.

4. В блоке параметров **Настройка GeoIP** нажмите на кнопку **Импортировать из файла** и выберите CSV-файл с геоданными.

   Дождитесь окончания импорта геоданных. При обновлении страницы загрузка данных прерывается.

Геоданные будут загружены в Kaspersky SIEM Cloud.

Чтобы экспортировать геоданные:

1. В веб-консоли откройте раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.
2. В блоке **Другое** нажмите **Общие**.
3. В блоке параметров **Настройка GeoIP** нажмите на кнопку **Экспортировать**.

   Геоданные будут скачаны в виде CSV-файла (в кодировке UTF-8) с названием `geoip.csv` в соответствии с параметрами вашего браузера.

Данные экспортируются в том же формате, в каком они были загружены, за исключением диапазонов IP-адресов. Если в Kaspersky SIEM Cloud в импортированном файле диапазон адресов указан в формате `1.0.0.0/24`, то в файле экспорта диапазон отображается в формате `1.0.0.0` - `1.0.0.255`.

Сопоставление геоданных по умолчанию

Если при настройке правила обогащения геоданными в качестве источника IP-адреса выбрать поля события `SourceAddress`, `DestinationAddress` и `DeviceAddress`, становится доступна кнопка **Применить сопоставление по умолчанию**. С ее помощью можно добавить преднастроенные пары соответствий атрибутов геоданных и полей события (см. таблицы ниже).

Соответствия по умолчанию для поля события SourceAddress

Атрибут геоданных	Поле события
Страна	`SourceCountry`
Регион	`SourceRegion`
Город	`SourceCity`
Широта	`SourceLatitude`
Долгота	`SourceLongitude`

Соответствия по умолчанию для поля события DestinationAddress

Атрибут геоданных	Поле события
Страна	`DestinationCountry`
Регион	`DestinationRegion`
Город	`DestinationCity`
Широта	`DestinationLatitude`
Долгота	`DestinationLongitude`

Соответствия по умолчанию для поля события DeviceAddress

Атрибут геоданных	Поле события
Страна	`DeviceCountry`
Регион	`DeviceRegion`
Город	`DeviceCity`

Атрибут геоданных	Поле события
Широта	`DeviceLatitude`
Долгота	`DeviceLongitude`

Получение и использование учетных записей Active Directory и Microsoft Entra ID

Kaspersky SIEM Cloud использует единый реестр учетных записей, в котором хранятся сведения об учетных записях Active Directory и Microsoft Entra ID. Для получения учетных записей Kaspersky SIEM Cloud использует Kaspersky Security Center Cloud Console, которая подключается к Active Directory и Microsoft Entra ID, получает сведения об учетных записях и передает их в Kaspersky SIEM Cloud через сервис Asset Manager.

Получение сведений из Kaspersky Security Center Cloud Console выполняется автоматически. Отдельно запускать получение учетных записей в Kaspersky SIEM Cloud не нужно.

Если сведения об одной учетной записи поступают из Active Directory и Microsoft Entra ID, они могут объединяться в одной карточке реестра. Учетные записи относятся к корневому тенанту рабочей области и не распределяются по дочерним тенантам на основании данных каталогов.

Настройка получения учетных записей

Чтобы учетные записи из Active Directory и Microsoft Entra ID стали доступны в Kaspersky SIEM Cloud:

1. Настройте точку распространения.

   Нужно назначить точкой распространения устройство, на котором настроен доступ к Active Directory и которое может взаимодействовать с контроллерами домена.

2. Настройте опрос контроллеров домена.

   Если используется точка распространения с операционной системой Windows, выберите один из следующих вариантов опроса:

   - **Опросить текущий домен**.
   - **Опросить весь лес доменов**.
   - **Опросить указанные домены**.

   Если используется точка распространения с операционной системой Linux, добавьте домен, указав адрес контроллера домена и учетные данные пользователя, а также выберите тип домена **Active Directory**.

3. При необходимости настройте расписание опроса контроллеров домена.

4. Убедитесь, что пользователи и группы из необходимых источников добавлены в Kaspersky Security Center Cloud Console.

   Если настроен опрос Active Directory и пользователи и группы вашей организации синхронизируются с Microsoft Entra ID из локальной Active Directory, они могут быть добавлены в Kaspersky Security Center Cloud Console в результате этого опроса.

Если нужные пользователи и группы не поступают из Active Directory, настройте опрос Microsoft Entra ID средствами Kaspersky Security Center Cloud Console.

5. Дождитесь получения учетных записей в Kaspersky SIEM Cloud.

После получения сведений из Kaspersky Security Center Cloud Console учетные записи автоматически становятся доступными в едином реестре Kaspersky SIEM Cloud. Полученные сведения сохраняются в Asset Manager и используются в Kaspersky SIEM Cloud.

Создание и использование учетных записей

Для создания или обновления карточки нужны идентификатор объекта, отображаемое имя и имя пользователя (UPN). Если UPN отсутствует, система пытается сформировать его из короткого имени учетной записи и домена, указанного в расположении записи. Если нужные сведения отсутствуют и UPN определить невозможно, карточка не создается или не обновляется.

Если сведения об одной учетной записи поступают из Active Directory и Microsoft Entra ID, система может объединить их в одной карточке. Для этого используется сопоставление по UPN в пределах корневого тенанта одной рабочей области. Уже существующие отдельные карточки автоматически не объединяются только на основании совпадения UPN.

В таблице ниже указаны данные, которые попадают в карточку учетной записи, если они присутствуют в источнике:

Данные, доступные в карточке учетной записи

Данные	Active Directory	Microsoft Entra ID
Идентификатор объекта	`objectGUID`	`id`
Идентификатор безопасности (SID)	`objectSid`	`securityIdentifier`, `onPremisesSecurityIdentifier`
Отображаемое имя	`displayName`	`displayName`
Расположение записи в каталоге (DN)	`distinguishedName`	`onPremisesDistinguishedName`
Имя учетной записи	`sAMAccountName`	`onPremisesSamAccountName`
Имя пользователя (UPN)	`userPrincipalName`	`userPrincipalName`
Электронная почта	`mail`	`mail`
Мобильный телефон	`mobile`	`mobilePhone`
Домен	Определяется по `distinguishedName` или `userPrincipalName`	Определяется по `userPrincipalName`, также может использоваться `onPremisesDomainName`
Группы учетной записи	`memberOf`	`memberOf`

Поля `onPremises*` относятся к сведениям, синхронизированным из Active Directory. Для учетных записей, созданных в Microsoft Entra ID, их наличие не гарантируется.

Если карточка содержит сведения из обоих каталогов, для подробных полей приоритет имеют данные Microsoft Entra ID. Если соответствующие сведения Entra ID отсутствуют, используются данные Active Directory. Пустое значение в полученных данных Entra ID не заменяется значением из AD. Отображаемое имя и UPN обновляются по последним непустым значениям.

Некоторые атрибуты каталогов, например должность, подразделение, рабочий телефон и руководитель, автоматически не получаются.

Сведения реестра можно использовать в следующих случаях:

- для просмотра карточек учетных записей;
- для поиска учетных записей и фильтрации результатов;
- для обогащения событий сведениями об учетных записях;
- для использования данных учетных записей в поисковых запросах, виджетах, отчетах и правилах корреляции.

Для сопоставления учетных записей с событиями можно использовать SID, имя учетной записи, UPN или адрес электронной почты. Сопоставление источника и назначения настраивается независимо. Архивные учетные записи при обогащении событий не используются.

Архивирование учетных записей

Если Kaspersky SIEM Cloud получает от Active Directory или Microsoft Entra ID сведения об удалении учетной записи, соответствующая карточка переводится в архив. Если одна карточка объединяет сведения из обоих каталогов, получение сообщения об удалении объекта из любого из них приводит к архивированию общей карточки.

Архивные учетные записи не удаляются немедленно. Они сохраняются в реестре для просмотра и анализа в течение установленного срока хранения.

Получение новых сведений об архивной учетной записи обновляет ее данные, но не возвращает ее автоматически в действующее состояние.

По умолчанию срок хранения архивных учетных записей составляет 90 дней. Срок хранения можно настроить для тенанта в пределах от 0 до 1024 дней. Значение 0 означает бессрочное хранение архивных записей. После истечения установленного срока архивная учетная запись автоматически удаляется.

Чтобы просмотреть и изменить срок хранения, нужно иметь права на **Чтение** и **Запись**.

Обогащение событий DNS-именами

Некоторые события, поступающие в Kaspersky SIEM Cloud, содержат IP-адреса. Для удобства чтения событий вам может понадобиться информация о том, каким DNS-именам соответствуют IP-адреса в событиях.

Для решения этой задачи вы можете использовать обогащение событий DNS-именами.

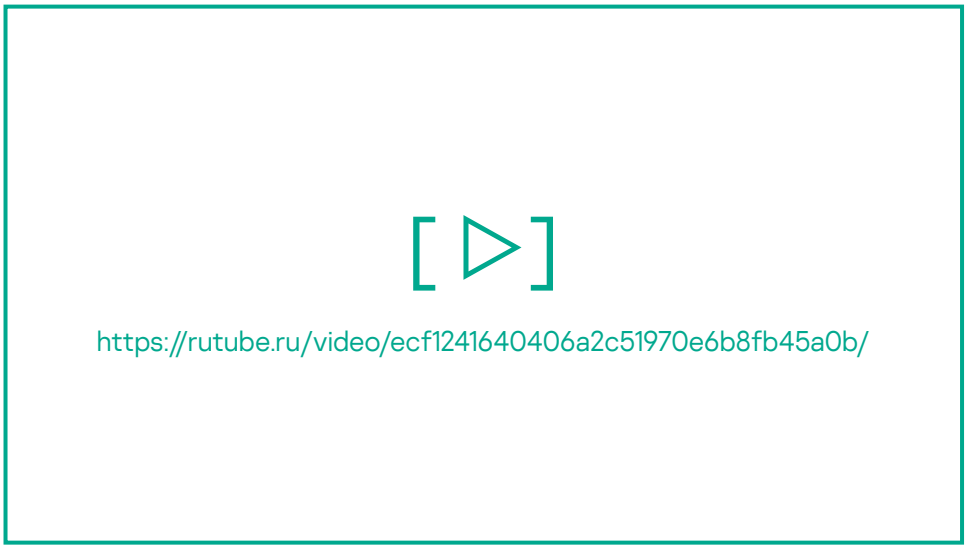
Чтобы настроить обогащение событий DNS-именами:

1. Создайте правило обогащения с типом **dns** одним из следующих способов:
   - на шаге **Обогащение событий** мастера установки коллектора;
   - в свойствах уже установленного коллектора в разделе **Обогащение событий**;
   - отдельно как ресурс.

2. Если вы создали правило обогащения DNS-именами отдельно как ресурс, добавьте его в свойствах коллекторов, обрабатывающих события с IP-адресами.

3. Обновите конфигурации коллекторов, к которым вы добавили правило обогащения DNS-именами.

Для наглядного ознакомления с обогащением событий данными с DNS-сервера вы можете просмотреть видео ниже.



https://rutube.ru/video/ecf1241640406a2c51970e6b8fb45a0b/

Обогащение событий с помощью словаря

В некоторых источниках событий значения полей событий передаются в виде кодов. При этом для анализа событий может понадобиться отображение описаний на соответствующие коды. Например, коду 1001 может соответствовать описание "Неудачная авторизация".

Для преобразования кодов в текстовые значения в Kaspersky SIEM Cloud можно использовать обогащение событий с помощью словаря. В словаре для каждого кода задается соответствующее ему значение. В нормализаторе настраивается правило обогащения с типом источника данных **словарь**.

При обработке события значение указанного поля используется в качестве ключевого поля для поиска соответствующей записи в словаре. Полученное из словаря значение записывается в указанное целевое поле нормализованного события. Например, если в исходном событии поле `event_code` содержит значение 1001, а в словаре этому коду соответствует значение "Неудачная авторизация", после обработки события поле `Name` будет содержать это значение.

Перед началом работы убедитесь, что выполнены следующие условия:

- Источник событий передает код в определенном поле, например `event_code`.
- В Kaspersky SIEM Cloud создан нормализатор для обработки событий источника.
- Подготовлен перечень кодов и соответствующих им описаний.

Настройка обогащения событий с помощью словаря состоит из следующих этапов:

1 Создание словаря

Словарь содержит пары Ключ – Значение. В качестве ключа используется код события, а в качестве значения – его описание.

Чтобы создать словарь:

1. В веб-интерфейсе перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Словари**.
2. Создайте словарь типа **Словарь**.
3. Добавьте в словарь записи, содержащие коды событий и соответствующие им описания.
4. Сохраните словарь.

Словарь может содержать следующие записи:

Примеры записей словаря

Ключ	Значение
1001	Неудачная авторизация
1002	Успешная авторизация
1003	Изменение пароля

В словаре должны быть указаны все коды, для которых нужно выполнять обогащение событий.

2 Настройка обогащения в нормализаторе

После создания словаря нужно настроить правило обогащения в нормализаторе.

Чтобы настроить правило обогащения:

1. В веб-интерфейсе Kaspersky SIEM Cloud перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Нормализаторы**.
2. Откройте параметры нормализатора, который обрабатывает события источника.
3. Перейдите на вкладку **Обогащение**.
4. Нажмите на кнопку **Добавить обогащение**.
5. В раскрывающемся списке **Тип источника данных** выберите **словарь**.
6. В поле **Название словаря** выберите созданный ранее словарь.
7. В раскрывающемся списке **Целевое поле** выберите поле **Name**.
8. В раскрывающемся списке **Ключевые поля** выберите поле исходного события, содержащее код события, например `event_code`.

9. При необходимости включите переключатель **Отладка**, чтобы добавить детализацию работы правила обогащения в журнал нормализатора.

10. Нажмите на кнопку **OK**.

11. Сохраните изменения нормализатора.

При обработке события значение поля `event_code` используется как ключ для поиска записи в выбранном словаре. Значение найденной записи записывается в поле `Name` нормализованного события. Например, если в исходном событии значение поля `event_code` – `1001`, а в словаре для ключа `1001` указано значение `Неудачная авторизация`, после обогащения поле `Name` нормализованного события будет содержать значение `Неудачная авторизация`.

3 Проверка работы обогащения событий

После настройки нужно отправить в Kaspersky SIEM Cloud тестовое событие, содержащее код, который присутствует в словаре.

Чтобы проверить работу обогащения:

1. Отправьте через коллектор тестовое событие, содержащее значение в поле `event_code`.

2. В веб-интерфейсе Kaspersky SIEM Cloud перейдите в раздел **События**.

3. Найдите обработанное тестовое событие.

4. Проверьте значение поля `Name`.

Если значение в поле `Name` отсутствует или отличается от ожидаемого, проверьте следующее:

- В словаре присутствует запись с соответствующим ключом.
- В раскрывающемся списке **Ключевые поля** выбрано поле, которое содержит код события.
- В качестве целевого поля указано поле `Name`.
- Измененный нормализатор сохранен и используется коллектором, обрабатывающим тестовое событие.

4 Обновление словаря (необязательный этап)

При добавлении новых кодов или изменении описаний обновите соответствующие записи словаря.

Чтобы обновить содержимое словаря:

1. В веб-интерфейсе Kaspersky SIEM Cloud перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Словари**.

2. Откройте словарь, используемый для обогащения.

3. Добавьте новые записи или измените существующие.

4. Сохраните изменения.

Настроенное в нормализаторе обогащение продолжит использовать этот словарь. Повторно создавать правило обогащения при изменении записей словаря необязательно. Kaspersky SIEM Cloud преобразует коды, указанные в исходных событиях, в соответствующие им текстовые значения и запишет их в поле `Name` нормализованного события.

Маршрутизация событий

Маршрутизатор событий – это сервис, который позволяет принимать потоки событий от коллекторов и коррелляторов и дальше распределять события по заданным точкам назначения в соответствии с настроенными фильтрами.

Чтобы события из коллектора были направлены в маршрутизатор событий, нужно создать ресурс точки назначения eventRouter с адресом маршрутизатора событий и привязать ресурс к тем коллекторам, которые должны отправлять события в маршрутизатор.

Маршрутизатор событий принимает события по API-порту, как и точки назначения типа storage и correlator.

Создать маршрутизатор можно в разделе **Мониторинг** → **Ресурсы и сервисы** → **Маршрутизаторы событий**.

Использование маршрутизатора событий позволяет снизить использование каналов связи, что актуально для каналов с невысокой пропускной способностью и каналов, уже загруженных продуктивным трафиком.

Маршрутизатор событий доступен для установки только на устройства под управлением Linux. Создавать сервис может только пользователь с ролью Главный администратор. Создавать сервис можно в любом тенанте, привязка к тенанту не накладывает никаких ограничений.

Вы можете установить сервис маршрутизатора событий как на отдельном хосте, так и вместе с коллектором или коррелятором. Поскольку для маршрутизатора событий в файле инвентаря отсутствует отдельная секция, вы можете указать хост для установки маршрутизатора событий в секции `kuma_collector` или `kuma_correlator`. Также если вы планируете устанавливать маршрутизатор событий на отдельном хосте, вам нужно указать этот хост в файле инвентаря в секции `kuma_collector` или `kuma_correlator`, тогда при очередном обновлении Kaspersky SIEM Cloud сервис маршрутизатора событий также будет обновлен.

Для получения информации о параметрах работы сервиса доступны следующие метрики:

- IO
- Process
- OS

Как и для прочих ресурсов, для маршрутизатора событий в Kaspersky SIEM Cloud создаются следующие события аудита:

- Ресурс успешно добавлен.
- Ресурс успешно обновлен.
- Ресурс успешно удален.

Установка маршрутизатора событий состоит из двух этапов:

- Создание сервиса маршрутизатора событий в веб-интерфейсе Kaspersky SIEM Cloud.
- Установка сервиса маршрутизатора событий на сервере.

Запуск мастера установки маршрутизатора событий

В Kaspersky SIEM Cloud есть предустановленный ресурс маршрутизатора событий [OOTB] OSMP Event Router. Вы можете либо создать новый ресурс маршрутизатора событий, либо воспользоваться предустановленным ресурсом.

Чтобы запустить мастер установки маршрутизатора событий:

1. В веб-консоли перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Маршрутизаторы событий**.
2. В открывшемся окне **Маршрутизаторы событий** нажмите **Добавить**.

Следуйте указаниям мастера установки.

Шаг 1. Общие параметры маршрутизатора событий

Это обязательный шаг мастера установки. На этом шаге вы указываете основные параметры маршрутизатора событий: название и тенант, которому он будет принадлежать.

Чтобы задать общие параметры маршрутизатора событий:

1. На вкладке **Основные параметры** заполните следующие поля:
   a. В поле **Название** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов в кодировке Unicode.
   b. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать маршрутизатор. Принадлежность маршрутизатора событий к тенанту носит организационный характер и не накладывает никаких ограничений.
   c. В поле **Обработчики** при необходимости укажите количество процессов, которые может одновременно запускать сервис. По умолчанию количество обработчиков соответствует количеству vCPU сервера, на котором установлен сервис.
   d. В поле **Описание** можно добавить описание сервиса: до 4000 символов в кодировке Unicode.
2. На вкладке **Дополнительные параметры** заполните следующие поля:
   a. При необходимости с помощью переключателя **Отладка** включите логирование операций сервиса.
   b. Переключатель **Периодическое создание дампа** используется по запросу Службы технической поддержки для генерации отчетов по потреблению ресурсов (cpu, ram и т.д.) в виде дампов.
   c. В поле **Настройки дампа** вы можете указать параметры создания дампа. Порядок заполнения этого поля уточняйте у Службы технической поддержки.

Общие параметры маршрутизатора событий заданы. Перейдите к следующему шагу мастера установки.

Шаг 2. Маршрутизация

Это обязательный шаг мастера установки. Мы рекомендуем отправлять события как минимум в две точки назначения: в коррелятор для анализа и в хранилище для хранения. Также вы можете выбрать другой маршрутизатор событий в качестве точки назначения.

Чтобы задать параметры точки назначения, куда маршрутизатор событий будет направлять события, полученные от коллекторов:

1. В шаге мастера установки **Маршрутизация** нажмите **Добавить**.

2. В открывшемся окне **Создание точки назначения** задайте следующие параметры:

   a. На вкладке **Основные параметры** в поле **Название** введите уникальное имя точки назначения. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   b. С помощью переключателя **Состояние** вы можете при необходимости включить или выключить сервис.

   c. В раскрывающемся списке **Тип** выберите тип точки назначения. Доступны следующие значения:

      - nats-jetstream
      - tcp
      - http
      - kafka
      - file
      - storage
      - correlator
      - eventRouter

   d. На вкладке **Дополнительные параметры** укажите значения для параметров настройки. Набор параметров для настройки зависит от типа точки назначения, выбранного на вкладке **Основные параметры**. Более подробная информация о параметрах и значениях доступна по ссылке для каждого типа точки назначения в пункте c. этой инструкции.

Созданная точка назначения отображается на вкладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

Параметры маршрутизации настроены. Вы можете перейти к следующему шагу мастера установки.

Шаг 3. Проверка параметров

Это обязательный и заключительный шаг мастера установки.

Чтобы создать маршрутизатор событий в мастере установки:

1. Нажмите **Сохранить и создать сервис**.

2. Закройте мастер, нажав **Сохранить**.

   Сервис будет установлен в веб-интерфейсе Kaspersky SIEM Cloud. Теперь вы можете перейти к установке сервиса в облачной инфраструктуре.

Пример использования: коллектор передает события на маршрутизатор в центре обработки данных

Коллектор передает события на маршрутизатор в центре обработки данных (ЦОД), а маршрутизатор передает события в заданные точки назначения: коррелятор и хранилище.

Компания состоит из нескольких филиалов. В ЦОД развернуты все компоненты Kaspersky SIEM Cloud. В филиалах развернуто несколько коллекторов. Каждый коллектор должен отправлять данные из филиала в хранилище и коррелятор в ЦОД. От некоторых филиалов до ЦОД нет широкополосного канала связи.

В этом случае вы можете установить в ЦОД маршрутизатор событий и направить поток данных от каждого коллектора в филиалах на маршрутизатор событий, а не напрямую в хранилище и коррелятор. Так как передача данных идет одним потоком, а не двумя, это снижает нагрузку на слабый канал связи.

Доставка событий в хранилище и коррелятор реализуется на стороне ЦОД. Для этого в свойствах маршрутизатора событий вам надо указать точки назначения хранилища и коррелятора.

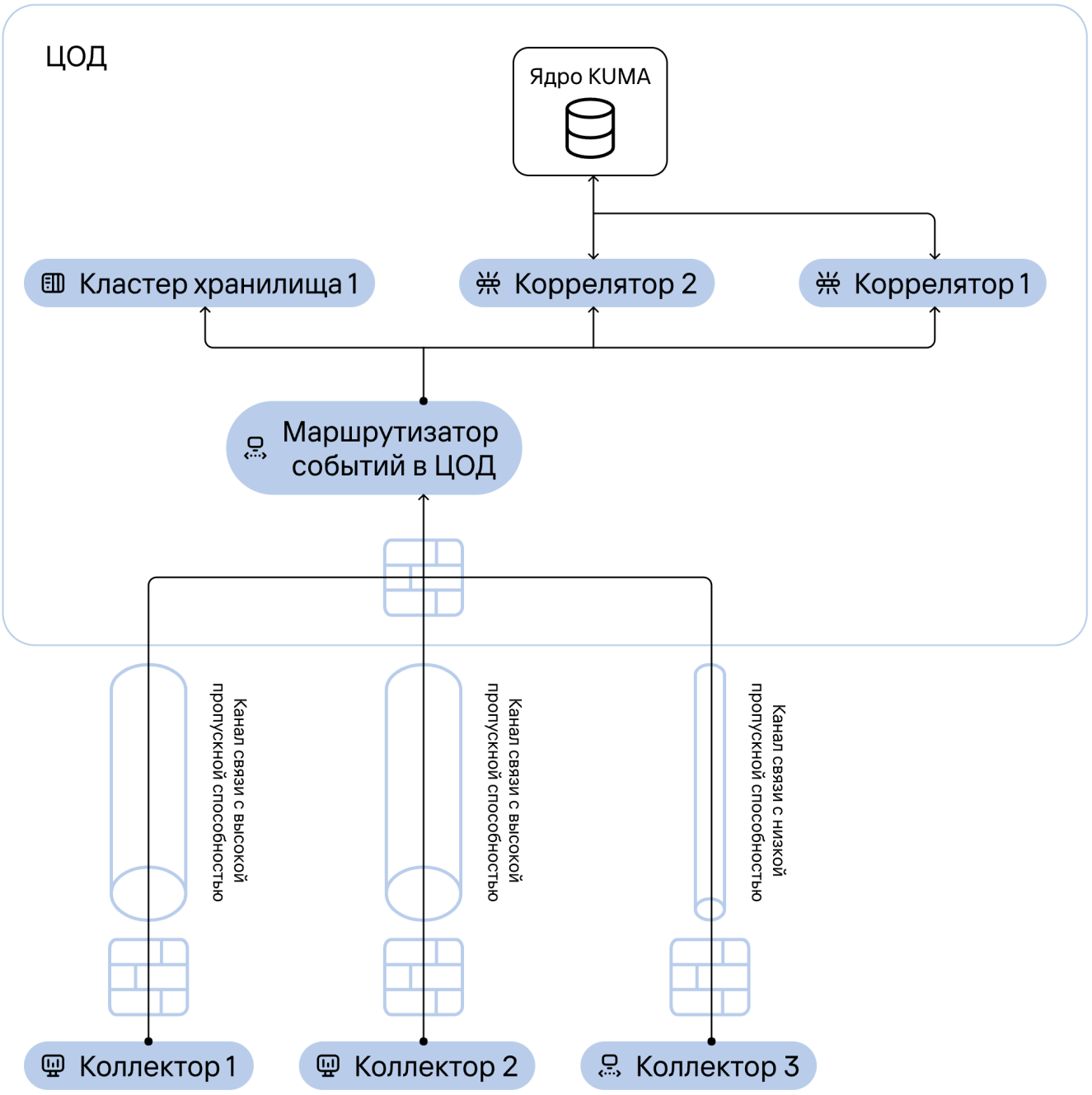


Схема подключения машрутизатора в ЦОД

Предусловия

- В филиалах настроены коллекторы.
- В ЦОД есть мощности для установки маршрутизатора событий.
- В ЦОД установлено Kaspersky SIEM Cloud.

Этапы

Настройка маршрутизатора событий состоит из следующих этапов:

1. **Создание точек назначения для хранилища и коррелятора**

   Если у вас еще не созданы точки назначения типа **storage** и **correlator** для хранилища и коррелятора в ЦОД, создайте их. В параметрах точек назначения укажите URL хранилища и URL коррелятора.

2. **Установка и настройка сервиса маршрутизатора событий в инфраструктуре ЦОД**

   Чтобы установить сервис маршрутизатора событий:

   1. Создайте сервис маршрутизатора событий в веб-интерфейсе Kaspersky SIEM Cloud. В разделе **Маршрутизация** добавьте точки назначения типа **storage** и **correlator** для хранилища и коррелятора в ЦОД.
   2. Установите сервис маршрутизатора событий на сервере.

3. **Создание точки назначения для маршрутизатора событий**

   Создайте точку назначения типа **eventRouter**. В параметрах точки назначения укажите URL маршрутизатора событий в ЦОД.

4. **Настройка коллекторов в филиалах для отправки событий в маршрутизатор событий в ЦОД**

   В свойствах коллекторов в разделе **Маршрутизация** укажите созданную точку назначения для маршрутизатора событий.

Данные из филиалов будут отправляться в ЦОД одним потоком, что снижает нагрузку на слабые каналы связи.

Пример использования: каскадное подключение маршрутизаторов событий

Несколько коллекторов передают события в маршрутизатор событий в филиале. Маршрутизатор событий в филиале передает события в маршрутизатор в центре обработки данных (ЦОД), где уже происходит передача событий в заданные точки назначения: коррелляторы и хранилище.

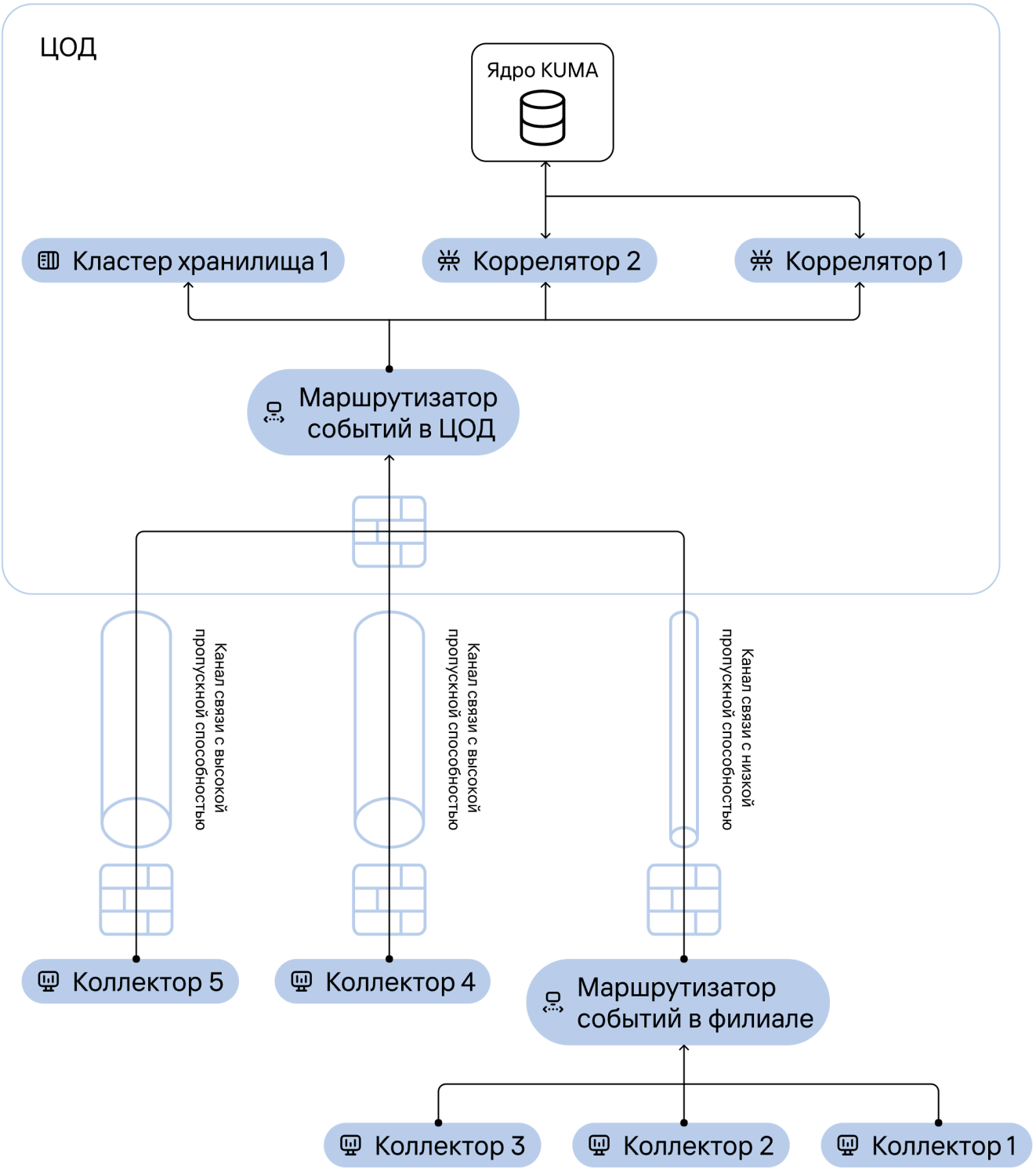


Схема каскадного подключения маршрутизаторов

Предусловия

- В филиалах настроены коллекторы.
- В центре обработки данных есть мощности для установки маршрутизатора событий.
- В центре обработки данных установлена Kaspersky SIEM Cloud.

Этапы

Настройка каскадного подключения маршрутизаторов событий состоит из следующих этапов:

1. **Настройка в центре обработки данных**

   В ЦОД вам нужно выполнить следующие действия:

   1. Создать сервис маршрутизатора событий.
   2. Создать точки назначения типа **storage** и **correlator** и указать их в маршрутизаторе событий.
   3. В маршрутизаторе событий на вкладке **Дополнительные параметры** настроить фильтр, чтобы передавать события в хранилище и/или коррелятор, например `DeviceCustomString` = `correlator` или `DeviceCustomString` = `storage`.

2. **Настройка в филиале**

   Для филиала нужно выполнить следующие действия:

   1. Создать сервис маршрутизатора событий.
   2. Создать точку назначения типа **eventRouter** и указать URL маршрутизатора событий в ЦОД.
   3. Для коллекторов филиалов создать точку назначения типа **eventRouter** и указать URL маршрутизатора событий в филиале.

      Если **eventRouter** заменяет собой прежде настроенные точки назначения, их можно удалить.

В ЦОД и филиалах будут настроены маршрутизаторы событий. Также в филиале будут настроены коллекторы.

Соединение филиалов с ЦОД оптимизировано. Теперь не требуется в каждом коллекторе настраивать отправку событий в центр обработки данных. Достаточно собрать общий поток событий на маршрутизатор и одним потоком отправить в центр обработки данных.

Создание и использование агентов Kaspersky SIEM Cloud

Агенты Kaspersky SIEM Cloud – это сервисы, которые используются для пересылки необработанных событий с серверов и рабочих станций в точки назначения Kaspersky SIEM Cloud.

Типы агентов:

- wmi – используются для получения данных с удаленных устройств Windows с помощью Windows Management Instrumentation. Устанавливается на устройства Windows.
- wec – используются для получения журналов Windows с локального устройства с помощью Windows Event Collector. Устанавливается на устройства Windows.
- tcp – используются для получения данных по протоколу TCP. Устанавливается на устройства Linux и Windows.
- udp – используются для получения данных по протоколу UDP. Устанавливается на устройства Linux и Windows.
- nats-jetstream – используются для коммуникации через NATS. Устанавливается на устройства Linux и Windows.
- kafka – используются для коммуникации с помощью kafka. Устанавливается на устройства Linux и Windows.
- http – используются для связи по протоколу HTTP. Устанавливается на устройства Linux и Windows.
- file – используются для получения данных из файла. Устанавливается на устройства Linux и Windows.
- ftp – используются для получения данных по протоколу File Transfer Protocol. Устанавливается на устройства Linux и Windows.
- nfs – используются для получения данных по протоколу Network File System. Устанавливается на устройства Linux и Windows.
- snmp – используются для получения данных с помощью Simple Network Management Protocol. Устанавливается на устройства Linux и Windows.
- diode – используются вместе с диодами данных для получения событий из изолированных сегментов сети. Устанавливается на устройства Linux и Windows.
- etw – используются для получения данных Event Tracing for Windows. Устанавливается на устройства Windows.

Создание агента состоит из следующих этапов:

1. Создание набора ресурсов агента в веб-интерфейсе
2. Создание сервиса агента в веб-интерфейсе
3. Установка серверной части агента на устройстве, с которого требуется передавать события

Агенты Kaspersky SIEM Cloud для устройств Windows можно создать следующим образом:

- Создать вручную путем создания набора ресурсов агента и создания сервиса агента в веб-интерфейсе Kaspersky SIEM Cloud.

- Создать автоматически при создании коллектора с типом транспорта wmi, wec или etw. Набор ресурсов и сервис таких агентов создаются в мастере установки коллектора, однако их все равно требуется установить на устройстве, с которого требуется передать события. В созданном вручную агенте коннектор с типом etw следует использовать только в одном подключении. Если вы настроите несколько подключений в созданном вручную агенте etw, статус агента etw будет зеленым, но события не будут передаваться и в журнале агента etw будет ошибка.

На одном устройстве может быть установлено несколько агентов, при этом все агенты должны быть одной версии.

Если на устройстве, где вы планируете создать агент, уже есть установленный агент более старой версии, требуется сначала остановить установленный агент (удалить агент с устройства Windows или перезапустить сервис агента для Linux), а затем можно создавать новый агент. При этом если установлены агенты той же версии, что и планируется создать, остановка агентов не требуется.

При создании и запуске агента версии 3.0.1 и более поздних версий требуется принять условия Лицензионного соглашения.

В конфигурации, где сервисы Ядра Kaspersky SIEM Cloud объединены в кластер Raft, все операции управления агентами (например, перезапуск) следует выполнять с того хоста, к которому агент подключен в текущий момент. Агент подключается к первому доступному Ядру Kaspersky SIEM Cloud из списка хостов, указанного в его конфигурации. Поэтому перед выполнением операции необходимо определить, к какому Ядру Kaspersky SIEM Cloud подключен агент, и выполнять операцию с соответствующего хоста. Например, если в конфигурации агента хосты перечислены в порядке 3, 2, 1, а хост 3 недоступен, агент подключится к Ядру Kaspersky SIEM Cloud на хосте 2. В этом случае все операции управления агентом необходимо выполнять с хоста 2.

Создание набора ресурсов для агента

Сервис агента создается на основе набора ресурсов для агента, в котором объединяются коннекторы и точки назначения. Типом агента считается тип использованного в нем коннектора. Исключением являются агенты с точкой назначения типа diode: такие агенты считаются diode-агентами.

Чтобы создать набор ресурсов для агента :

1. В веб-консоли перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Агенты** нажмите **Создать**.

   Откроется окно создания агента. В левой части окна отображаются вкладки с общими параметрами агента и подключениями. Вкладка **Общие параметры** будет активна.

2. На вкладке **Общие параметры** выполните следующие действия:

   - В поле **Название** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   - В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать хранилище.

   - Если требуется включить логирование операций сервиса, переведите переключатель **Отладка** в активное положение.

- Если требуется просматривать имена сервисов или адреса хостов, откуда приходит событие, переведите переключатель **Отслеживать маршрут события** в активное положение.

  Переключатель **Отслеживать маршрут события** доступен, если в подключениях указана хотя бы одна точка назначения с типом **internal**. По умолчанию переключатель находится в положении **Выключено**.

- В поле **Описание** при необходимости добавьте описание сервиса: до 256 символов в кодировке Unicode.

3. Перейдите на вкладку существующего подключения или создайте подключение с помощью кнопки **Добавить** в нижней части панели слева и переключитесь на вкладку созданного подключения, чтобы изменить его параметры.

   По умолчанию для нового агента создается подключение **Подключение №1**. Новому подключению присваивается название по шаблону **Подключение <номер>**.

   Вы можете создать несколько подключений для агента. При необходимости вы можете управлять подключениями:

   - переименовывать подключения;
   - дублировать подключения;
   - удалять подключения.

4. При необходимости в поле **Название подключения** переименуйте подключение для более удобной работы с ними, например, чтобы определить, от какого подключения и с какого агента пришли события. Если вы оставите поле пустым, будет использовано название по шаблону **Подключение <номер>**.

   Длина названия может быть от 1 до 128 символов. Название может содержать только буквы и цифры и не может содержать специальные символы. Пробелы в начале и конце строки названия будут удалены. При вставке названия в поле из буфера обмена, если текст содержит перенос строки, абзац или отступ, эти символы будут заменены на пробел. Вы можете использовать одинаковое название для нескольких подключений внутри одного агента.

   Если вы включили отслеживание маршрута события, то при просмотре информации о событии в разделе **События** будет отображаться название подключения, от которого пришло это событие.

5. В блоке параметров **Коннектор** добавьте коннектор:

   - Если хотите выбрать существующий коннектор, выберите его в раскрывающемся списке.
   - Если хотите создать новый коннектор, выберите в раскрывающемся списке **Создать** и укажите следующие параметры:
     - В поле **Название** укажите имя коннектора. Название должно содержать от 1 до 128 символов в кодировке Unicode.
     - В раскрывающемся списке **Тип** выберите тип коннектора и укажите его параметры на вкладках **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа коннектора:
       - tcp
       - udp
       - nats-jetstream
       - kafka

- http
- file
- ftp
- nfs
- wmi
- wec
- snmp
- snmp-trap
- etw
- kata/edr
- office365
- dfi
- vmware
- 1c-log
- 1c-xml

При использовании типа коннектора **tcp**, **udp**, **http**, **wec**, **wmi**, **etw** на этапе нормализации в поле событий DeviceAddress, если оно пустое, будут записаны IP-адреса устройств, с которых были получены события.

Возможности по изменению уже созданных wec-. wmi- или etw-подключений в агентах, коллекторах и коннекторах ограничены. Тип подключения можно изменить с **wec** на **wmi** или **etw** обратно, однако типы **wec**, **wmi** и **etw** не получится сменить на какой-либо другой тип подключения. При этом при изменении других типов подключений невозможно выбрать типы **wec**, **wmi** и **etw**. Новые подключения можно создавать без ограничения по типам коннекторов.

При добавлении коннектора типа wmi, wec или etw (существующего или нового) для агента параметры **Режим TLS** и **Сжатие** не будут отображаться на агенте, но их значения будут храниться в его конфигурации. Для нового коннектора эти параметры по умолчанию выключены.
Если для существующего коннектора, выбранного из списка, режим TLS включен, вы не сможете скачать файл конфигурации агента. В этом случае, чтобы скачать файл конфигурации, необходимо перейти в ресурс коннектора, который используется на агенте, и отключить режим TLS.

Коннектор добавлен в выбранное подключение набора ресурсов агента. Созданный коннектор доступен только в этом наборе ресурсов и не отображается в разделе веб-интерфейса **Ресурсы** → **Коннекторы**.

6. В блоке параметров **Точки назначения** добавьте точку назначения.

   - Если хотите выбрать существующую точку назначения, выберите ее в раскрывающемся списке.
   - Если хотите создать новую точку назначения, выберите в раскрывающемся списке **Создать** и укажите следующие параметры:
     - В поле **Название** укажите имя точки назначения. Название должно содержать от 1 до 128 символов в кодировке Unicode.
     - В раскрывающемся списке **Тип** выберите тип точки назначения и укажите ее параметры на вкладках **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа точки назначения:
       - **nats-jetstream** – используется для коммуникации через NATS.
       - **tcp** – используется для связи по протоколу TCP.
       - **http** – используется для связи по протоколу HTTP.
       - **diode** – используется для передачи событий с помощью диода данных.
       - **kafka** – используется для коммуникаций с помощью kafka.
       - **file** – используется для записи в файл.
   - Включите или выключите переключатель **Состояние**, чтобы включить или выключить отправку событий в точку назначения. По умолчанию этот переключатель включен.

   > Дополнительные параметры точки назначения агента (например, сжатие и режим TLS) должны совпадать с дополнительными параметрами точки назначения коллектора, с которым вы хотите связать агент.

   Точек назначения может быть несколько. Их можно добавить с помощью кнопки **Добавить точку назначения** и удалить с помощью кнопки ✕.

7. Повторите шаги 3–5 для каждого подключения агента, которое вы хотите создать.

8. Нажмите **Сохранить**.

Набор ресурсов для агента создан и отображается в разделе **Ресурсы и сервисы** → **Агенты**. Теперь можно создать сервис агента.

Управление подключениями для агента

Вы можете управлять созданными для агента подключениями: переименовывать, дублировать или удалять их.

Переименование подключения

По умолчанию новому подключению, созданному в наборе ресурсов для агента, присваивается название по шаблону **Подключение <номер>**. Для более удобной работы с подключениями вы можете переименовывать их, например, чтобы определить, от какого подключения и какого агента пришли события.

Чтобы переименовать подключение:

1. В веб-консоли в разделе **Мониторинг** → **Ресурсы и сервисы** → **Агенты** создайте новый агент или нажмите на существующий агент в таблице.
2. При необходимости создайте подключение для агента с помощью кнопки **Добавить** в нижней части панели слева.
3. Перейдите на вкладку подключения, которое вы хотите переименовать.
4. В поле **Название подключения** измените название подключения.

   Длина названия может быть от 1 до 128 символов. Название может содержать только буквы и цифры и не может содержать специальные символы. Пробелы в начале и конце строки названия будут удалены. При вставке названия в поле из буфера обмена, если текст содержит перенос строки, абзац или отступ, эти символы будут заменены на пробел. Вы можете использовать одинаковое название для нескольких подключений внутри одного агента.
5. Нажмите **Сохранить**.

Подключение переименовано. Если вы включили отслеживание маршрута события, то при просмотре информации о событии в разделе **События** будет отображаться название подключения, от которого пришло это событие.

Дублирование подключения

Если вы хотите создать подключение для агента на основе существующего подключения, вы можете создать копию подключения с теми же параметрами.

Чтобы дублировать подключение:

1. В веб-консоли в разделе **Мониторинг → Ресурсы и сервисы → Агенты** создайте новый агент или нажмите на существующий агент в таблице.
2. При необходимости создайте подключение для агента с помощью кнопки **Добавить** в нижней части панели слева.
3. Перейдите на вкладку подключения, которое вы хотите дублировать, и нажмите на кнопку **Дублировать**.

Для агента будет создано подключение с такими же параметрами, как в исходном подключении. Новое подключение будет создано с одним из следующих названий:

- Если название исходного подключения соответствовало шаблону **Подключение <номер>**, название дублированного подключения также будет соответствовать этому шаблону. Подключению будет присвоен номер <номер>+1 от номера последнего созданного подключения с названием по такому же шаблону.
- Если исходное подключение ранее было переименовано, новое подключение будет создано с таким же названием. Вы можете использовать одинаковое название для нескольких подключений внутри одного агента.

Вы можете изменить название нового подключения в поле **Название подключения** на вкладке этого подключения.

Удаление подключения

Если для агента создано более одного подключения, вы можете удалить подключение.

Чтобы удалить подключение:

1. В веб-консоли в разделе **Мониторинг → Ресурсы и сервисы → Агенты** создайте новый агент или нажмите на существующий агент в таблице.
2. При необходимости создайте подключение для агента с помощью кнопки **Добавить** в нижней части панели слева.
3. Перейдите на вкладку подключения, которое вы хотите удалить, и нажмите на кнопку **Удалить**.

Вы не сможете восстановить подключение после удаления, но вы можете восстановить версию агента, в которой ранее было сохранено это подключение, через историю изменений.

Создание сервиса агента в веб-консоли

Когда набор ресурсов для агента создан, можно перейти к созданию сервиса агента в веб-консоли.

Чтобы создать сервис агента в веб-консоли:

1. В веб-консоли перейдите в раздел **Мониторинг**→ **Ресурсы и сервисы** → **Активные сервисы** и нажмите **Добавить сервис**.

2. В открывшемся окне **Выберите сервис** выберите только что созданный набор ресурсов для агента и нажмите **Создать сервис**.

Сервис агента создан и отображается в разделе **Ресурсы и сервисы** → **Активные сервисы**. Теперь сервисы агента необходимо установить на каждом устройстве, с которого вы хотите передавать данные в коллектор. При установке используется идентификатор сервиса.

Автоматически созданные агенты

При создании коллектора с коннекторами типа wec, wmi или etw автоматически создаются агенты для приема событий Windows.

Автоматически созданные агенты имеют ряд особенностей:

- Автоматически созданные агенты могут иметь только одно подключение.
- Автоматически созданные агенты отображаются в разделе **Мониторинг** → **Ресурсы и сервисы** → **Агенты**, в конце их названия указаны слова `auto created`. Агенты можно просмотреть или удалить.
- Параметры автоматически созданных агентов указываются автоматически на основе параметров коллектора из разделов **Подключение источников** и **Транспорт**. Изменить параметры можно только в коллекторе, для которого был создан агент.
- В качестве описания автоматически созданного агента используется описание коллектора в разделе **Подключение источников**.
- Отладка автоматически созданного агента включается и выключается в разделе коллектора **Подключение источников**.
- При удалении коллектора с автоматически созданным агентом вам будет предложено удалить коллектор вместе с агентом или удалить только коллектор. При удалении только коллектора агент станет доступен для редактирования.
- При удалении автоматически созданных агентов тип коллектора меняется на **http**, а из поля **URL** коллектора удаляется адрес подключения.
- Если хотя бы одно название журнала Windows указано в коннекторе типа wec или wmi с ошибкой, агент не будет получать события из всех перечисленных в коннекторе журналов Windows. При этом статус агента будет зеленый. Попытки получить события будут повторяться каждые 60 секунд, сообщения об ошибке будут добавляться в журнал сервиса.
- Если в коннекторе типа etw имя сессии указано некорректно, указан не тот провайдер в сессии или указан неверный способ, в каком режиме отправлять события (для корректной отправки событий на стороне Windows Server должен быть указан режим Real time или File and Real time), от агента не будут поступать события, в журнале агента на Windows будет зарегистрирована ошибка, а статус агента будет зеленым. При этом попытки получить события каждые 60 сек не будет. Если вы изменяете параметры сессии на стороне Windows, следует перезапустить агент etw и/или сессию, чтобы изменения были применены.

В веб-консоли автоматически созданные агенты появляются одновременно с созданием коллектора, однако их все равно требуется установить на устройстве, с которого требуется передать сообщение.

Установка агента в сетевой инфраструктуре OSMP

Когда сервис агента создан в OSMP, можно перейти к установке агента на устройствах сетевой инфраструктуры, с которых вы хотите передавать данные в коллектор.

На одном устройстве может быть установлено несколько агентов, при этом все агенты должны быть одной версии.

Перед установкой убедитесь в сетевой связности системы и откройте используемые компонентами порты.

Установка агента Kaspersky SIEM Cloud на устройствах Linux

Агент Kaspersky SIEM Cloud, установленный на устройствах Linux, останавливается при закрытии терминала или при перезапуске сервера. Если вы не хотите запускать агенты Kaspersky SIEM Cloud вручную, мы рекомендуем устанавливать их с помощью программы, которая автоматически запускает программы при перезапуске сервера, например с помощью программы Supervisor. Если вы хотите запускать агенты Kaspersky SIEM Cloud автоматически, укажите в конфигурационном файле Kaspersky SIEM Cloud параметры автоматического запуска и перезапуска. Подробнее о настройке параметров автоматического запуска и перезапуска см. официальную документацию программ для автоматического запуска программ.

Пример настройки параметров в программе Supervisor

```
[program:agent_<agent_name>] command=sudo /opt/kaspersky/kuma/agent agent --core https://<FQDN>:<port>
autostart=true
autorestart=true
```

где:

- <agent_name> - имя агента Kaspersky SIEM Cloud.
- <FQDN> - полное доменное имя сервера Ядра Kaspersky SIEM Cloud.
- <port> - номер порта Ядра Kaspersky SIEM Cloud.

Чтобы установить агент Kaspersky SIEM Cloud на устройство Linux:

1. На устройстве Linux, на котором вы хотите установить агент Kaspersky SIEM Cloud, создайте директории для конфигурационного файла и агентов Kaspersky SIEM Cloud, например:
   - /opt/kaspersky/kuma;
   - /opt/kaspersky/agent.

2. Поместите конфигурационный файл Kaspersky SIEM Cloud в созданную для него директорию. Конфигурационный файл Kaspersky SIEM Cloud расположен внутри установщика в директории /kuma-ansible-installer/roles/kuma/files.

   Убедитесь, что файл kuma имеет достаточные права для запуска.

3. Создайте пользователя Kaspersky SIEM Cloud выполнив команду:

   ```
   sudo useradd --system kuma && usermod -s /usr/bin/false kuma
   ```

4. Предоставьте пользователю Kaspersky SIEM Cloud доступ к директории с конфигурационным файлом Kaspersky SIEM Cloud, а также ко всем файлам внутри директории, выполнив команду:

   ```
   sudo chown -R kuma:kuma <path>
   ```

   где:

   <path> — путь к директории с конфигурационным файлом Kaspersky SIEM Cloud.

5. Установите агент Kaspersky SIEM Cloud, выполнив команду:

   ```
   sudo /opt/kaspersky/kuma/agent agent --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id
   <service_ID> --wd <path> [--accept-eula]
   ```

   где:

   - <FQDN> — полное доменное имя сервера Ядра Kaspersky SIEM Cloud.
   - <port> — номер порта Ядра Kaspersky SIEM Cloud для внутренних коммуникаций (по умолчанию используется порт 7210).
   - <CA_cert_ID> — идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса. Параметр `--pair.fingerprint` является необязательным.

     Вы можете выполнить установку сервиса без указания параметра `--pair.fingerprint`. В этом случае Kaspersky SIEM Cloud использует значение `insecure` по умолчанию, что не обеспечивает проверку подлинности CA-сертификата Ядра Kaspersky SIEM Cloud при установлении соединения. Если используется значение `insecure`, обновление отпечатка после перевыпуска CA-сертификата не требуется.

     Если вы хотите указать идентификатор отпечатка для обеспечения проверки подлинности CA-сертификата Ядра Kaspersky SIEM Cloud, перейдите в раздел **Ресурсы и сервисы** → **Активные сервисы**, установите флажок рядом с сервисом Ядра Kaspersky SIEM Cloud, в меню (⋮) выберите **Копировать отпечаток сертификата**, затем скопированный идентификатор используйте в команде установки агента. При перевыпуске CA-сертификата необходимо скопировать новый отпечаток сертификата в веб-интерфейсе и перезапустить сервис с обновленным значением параметра.

   - <service_ID> — идентификатор сервиса, скопированный из веб-интерфейса Kaspersky SIEM Cloud.
   - <path> — путь к директории, где будут размещаться файлы устанавливаемого агента Kaspersky SIEM Cloud. Если не указать этот параметр, файлы будут храниться в директории, где расположен файл kuma.

Вы можете установить два агента Kaspersky SIEM Cloud на одном устройстве Linux. В этом случае агенты Kaspersky SIEM Cloud будут работать параллельно. При установке второго агента Kaspersky SIEM Cloud вам нужно указать для него отдельную директорию с помощью параметра `--wd`.

Для запуска агента вам нужно принять Лицензионное соглашение. Вы можете добавить в команду параметр `--accept-eula`, чтобы автоматически принять Лицензионное соглашение во время установки агента Kaspersky SIEM Cloud. В этом случае установка не требует интерактивного взаимодействия. Если вы не укажете этот параметр, вам нужно будет принять или отклонить Лицензионное соглашение самостоятельно во время установки агента Kaspersky SIEM Cloud.

Примеры установки агента Kaspersky SIEM Cloud:

- Установка агента Kaspersky SIEM Cloud без автоматического принятия Лицензионного соглашения:

```
sudo /opt/kaspersky/kuma/agent agent --core https://kuma.example.com:7210 --id XXXX --wd
/opt/kaspersky/kuma/agent/XXXX
```

- Установка агента Kaspersky SIEM Cloud с автоматическим принятием Лицензионного соглашения:

```
sudo /opt/kaspersky/kuma/agent agent --core https://kuma.example.com:7210 --id XXXX --wd
/opt/kaspersky/kuma/agent/XXXX --accept-eula
```

Используя параметр `--accept-eula` во время установки агента Kaspersky SIEM Cloud, вы подтверждаете, что согласны с условиями Лицензионного соглашения и принимаете их.

6. Если вы выбрали установку Kaspersky SIEM Cloud с автоматическим принятием Лицензионного соглашения и хотите ознакомиться текстом лицензии или в процессе установки вам не был автоматически предоставлен текст Лицензионного соглашения, выполните команду:

```
./agent license --show
```

Агент Kaspersky SIEM Cloud будет установлен на устройстве Linux.

Вы можете настроить коллектор для приема данных, которые агент Kaspersky SIEM Cloud пересылает в Kaspersky SIEM Cloud.

Установка агента Kaspersky SIEM Cloud на устройствах Windows

Перед установкой агента Kaspersky SIEM Cloud на устройстве Windows убедитесь, что учетная запись, под которой будет запускаться агент Kaspersky SIEM Cloud, обладает необходимыми правами.

Права для учетной записи при установке агента Kaspersky SIEM Cloud любого типа

Администратору сервера необходимо создать на устройстве Windows учетную запись с правом Log on as a service. Эту учетную запись необходимо использовать для установки агента.

Права для учетной записи при установке агента Kaspersky SIEM Cloud типа wec

Администратору сервера необходимо создать на устройстве Windows учетную запись с правами Event Log Readers и Log on as a service. Эту учетную запись необходимо использовать для установки и запуска агента.

Если вы планируете получать события из журнала Security на контроллере домена, предоставьте предустановленной в Windows учетной записи Network Service доступ к журналу Security. Для этого на устройстве контроллера домена в командной строке PowerShell выполните команду:

```
wevtutil sl security /ca:'O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)
(A;;0x1;;;S-1-5-20)'
```

> Если вы не настроите доступ к журналу Security, но в параметрах коннектора wec добавите журнал Security, то поток событий от агента Kaspersky SIEM Cloud поступать не будет.

Если вы планируете получать события не с контроллера домена, достаточно добавить предустановленную в Windows учетную запись Network Service в группу Event Log Readers.

Права для учетной записи при установке агента Kaspersky SIEM Cloud типа wmi

Администратору сервера необходимо создать на устройстве Windows учетную запись с правами Event Log Readers и Log on as a service. Эту учетную запись необходимо использовать для установки агента.

Для запуска агента под доменной учетной записью необходимы права Event Log Readers и Log on as a service.

Если вы хотите запустить агент под локальной учетной записью, для запуска потребуются права администратора, а также права Event Log Readers и Log on as a service.

Если вы хотите выполнить удаленный сбор событий (сбор событий с устройств, подключенных к устройству, на котором установлен агент Kaspersky SIEM Cloud) и только чтение журналов под доменной учетной записью, будет достаточно права Event Log Readers.

Права для учетной записи при установке агента Kaspersky SIEM Cloud типа etw

Администратору сервера необходимо создать на устройстве Windows учетную запись с правом Log on as a service. Эту учетную запись необходимо использовать для установки агента.

Для запуска агента учетная запись должна обладать правами администратора или должна быть добавлена в одну из групп безопасности:

- Domain admins
- Performance Log Users

Установка агента Kaspersky SIEM Cloud

Чтобы установить агент Kaspersky SIEM Cloud на устройство Windows:

1. Скопируйте файл kuma.exe в папку на устройстве Windows. Для установки рекомендуется использовать папку `C:\Users\<имя пользователя>\Desktop\KUMA`.

   Файл kuma.exe находится внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

2. Запустите командную строку на устройстве Windows с правами администратора и найдите папку с файлом kuma.exe.

3. Выполните следующую команду:

```
kuma agent --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id <service_ID> --user <user> --
install [--accept-eula]
```

где:

- <FQDN> — полное доменное имя сервера Ядра Kaspersky SIEM Cloud.
- <port> — номер порта Ядра Kaspersky SIEM Cloud для внутренних коммуникаций (по умолчанию используется порт 7210).
- <CA_cert_ID> — идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса. Параметр `--pair.fingerprint` является необязательным.

  Вы можете выполнить установку сервиса без указания параметра `--pair.fingerprint`. В этом случае Kaspersky SIEM Cloud использует значение `insecure` по умолчанию, что не обеспечивает проверку подлинности CA-сертификата Ядра Kaspersky SIEM Cloud при установлении соединения. Если используется значение `insecure`, обновление отпечатка после перевыпуска CA-сертификата не требуется.

  Если вы хотите указать идентификатор отпечатка для обеспечения проверки подлинности CA-сертификата Ядра Kaspersky SIEM Cloud, перейдите в раздел **Ресурсы и сервисы** → **Активные сервисы**, установите флажок рядом с сервисом Ядра Kaspersky SIEM Cloud, в меню (⋮) выберите **Копировать отпечаток сертификата**, затем скопированный идентификатор используйте в команде установки агента. При перевыпуске CA-сертификата необходимо скопировать новый отпечаток сертификата в веб-интерфейсе и перезапустить сервис с обновленным значением параметра.
- <service_ID> — идентификатор сервиса, скопированный из веб-интерфейса Kaspersky SIEM Cloud.
- <user> — имя пользователя, под которым будет работать агент, включая домен.

Для запуска агента вам нужно принять Лицензионное соглашение. Вы можете добавить в команду параметр `--accept-eula`, чтобы автоматически принять Лицензионное соглашение во время установки агента. В этом случае установка не требует интерактивного взаимодействия. Если вы не укажете этот параметр, вам нужно будет принять или отклонить Лицензионное соглашение самостоятельно во время установки агента Kaspersky SIEM Cloud.

Примеры:

- Установка агента Kaspersky SIEM Cloud без автоматического принятия Лицензионного соглашения:

  ```
  kuma agent --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --user domain\username -
  -install
  ```

- Установка агента Kaspersky SIEM Cloud с автоматическим принятием Лицензионного соглашения:

  ```
  kuma agent --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --user domain\username -
  -install --accept-eula
  ```

Используя параметр `--accept-eula` во время установки агента Kaspersky SIEM Cloud, вы подтверждаете, что согласны с условиями Лицензионного соглашения и принимаете их.

Справочная информация об установщике доступна по команде `kuma help agent`.

4. Если вы запустили установку агента без автоматического принятия Лицензионного соглашения, в процессе установки вам будет предложено ознакомиться с текстом лицензии и у вас будет возможность принять соглашение или отказаться.

5. Если вы выбрали установку с автоматическим принятием Лицензионного соглашения и хотите ознакомиться текстом лицензии или в процессе установки вам не был автоматически предоставлен текст Лицензионного соглашения, выполните следующую команду:

   ```
   kuma.exe license --show
   ```

   Если вы хотите принять Лицензионное соглашение, выполните следующую команду и нажмите `y`:

   ```
   kuma.exe license
   ```

6. Укажите пароль для пользователя, под которым будет работать агент одним из следующих способов:

   - Вручную.
   - Из файла при установке агента.

     Чтобы не вводить пароль вручную, добавьте пароль в файл в формате .TXT и разместите файл в той же директории, что и бинарный файл агента.

     Укажите в команде содержащий пароль файл следующим образом: `<name of the file containing the password>.txt`. Например, `password.txt`.

     ```
     kuma agent --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --user domain\username --install  < password.txt
     ```

     Все данные из файла password.txt будут перенаправлены в команду в качестве пароля, за исключением символов конца строки (\n\r , \n).

     Путь хранения папки с агентом после установки: C:\ProgramData\Kaspersky Lab\KUMA\agent\${agent_id}.

   Если лицензионное соглашение (EULA) не было принято перед установкой агента с флагом `< password.txt`, появится ошибка с сообщением, о том что соглашение не принято.

   Варианты принятия EULA:

   a. В файле с паролем можно указать признак принятия EULA. Для этого в файле с паролем должны быть две строки: первая с признаком принятия EULA "y", вторая - с паролем. Например:

      `y`

      `<password>`

      Команда установки агента будет выглядеть следующим образом:

      ```
      kuma agent --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --user domain\username --install < password.txt
      ```

      В этом случае при установке агента дополнительно принимать EULA не потребуется.

Если ранее, до запуска команды с файлом-паролем, была принята EULA, первая строка в файле будет воспринята как пароль и установка завершится ошибкой `Access denied`.

b. Можно принять EULA и выполнить тихую установку одновременно, применив флаг --accept-eula.

Команда установки агента будет выглядеть следующим образом:

```
kuma agent --core https://kuma.example.com:7210 --pair.fingerprint XXXX --id XXXXX --user domain\username --accept-eula --install < password.txt
```

При этом важно, чтобы в файле был указан только пароль первой строкой, иначе возникнет ошибка.

Создана папка `C:\ProgramData\Kaspersky Lab\KUMA\agent\<agent ID>`, в нее установлен сервис агента Kaspersky SIEM Cloud. Агент пересылает события Windows в Kaspersky SIEM Cloud: можно настроить коллектор для их приема.

Когда сервис агента установлен, он запускается автоматически. Сервис также настроен на перезапуск в случае сбоев. Агент можно перезапустить из веб-интерфейса Kaspersky SIEM Cloud, но только когда сервис активен. В противном случае сервис требуется перезапустить вручную на машине Windows.

Удаление агента Kaspersky SIEM Cloud с устройств Windows

Чтобы удалить агент Kaspersky SIEM Cloud с устройства Windows:

1. Запустите командную строку на компьютере Windows с правами администратора и найдите папку с файлом kuma.exe.

2. Выполните любую из команд ниже:

   - `kuma.exe agent --cfg <путь к файлу конфигурации агента> --uninstall`

   - `kuma.exe agent --id <идентификатор сервиса агента, созданного в Kaspersky SIEM Cloud> --uninstall`

Указанный агент Kaspersky SIEM Cloud удален с устройства Windows. События Windows больше не отправляются в Kaspersky SIEM Cloud.

При настройке сервисов можно проверить конфигурацию на наличие ошибок до установки, запустив агент с помощью команды:

```
kuma agent --core https://<FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id <service_ID> --user <user>
```

Обновление агентов

При обновлении версий Kaspersky SIEM Cloud требуется обновить и установленные на удаленных машинах агенты WMI, WEC и ETW.

Чтобы обновить агент, используйте учетную запись с правами администратора и выполните следующие шаги:

1. В ОС Windows в разделе **Службы** откройте агент и нажмите **Стоп**.

2. В командном интерпретаторе перейдите в папку, где был установлен агент и выполните команду по удалению агента с сервера.

   ```
   kuma.exe agent --id <agent_ID> --uninstall
   ```

   где:

   <agent_ID> — идентификатор сервиса агента, созданного в Kaspersky SIEM Cloud.

3. Поместите в ту же папку новый агент.

4. В командном интерпретаторе перейдите в папку с новым агентом и из этой папки выполните команду установки, используя идентификатор агента из пункта 1.

   ```
   kuma agent --core <FQDN>:<port> --pair.fingerprint <CA_cert_ID> --id <agent_ID> --user <user> --install
   ```

   где:

   - <FQDN> — полное доменное имя сервера Ядра KUMA.
   - <port> — порт, используемый сервером Ядра KUMA для внутренних коммуникаций (по умолчанию используется порт 7210).
   - <CA_cert_ID> — идентификатор отпечатка CA-сертификата, используемый для проверки подлинности при подключении сервиса.

     Параметр `--pair.fingerprint` является необязательным. При создании сервиса Kaspersky SIEM Cloud автоматически добавляет этот параметр в команду установки и указывает идентификатор отпечатка.
     Вы можете выполнить установку сервиса без указания параметра `--pair.fingerprint`. В этом случае Kaspersky SIEM Cloud использует значение `insecure` по умолчанию, что не обеспечивает проверку подлинности CA-сертификата Ядра Kaspersky SIEM Cloud при установлении соединения. Если используется значение `insecure`, обновление отпечатка после перевыпуска CA-сертификата не требуется.

     Для обеспечения проверки подлинности CA-сертификата Ядра Kaspersky SIEM Cloud рекомендуется не удалять параметр `--pair.fingerprint` с идентификатором отпечатка при установке сервиса. При перевыпуске CA-сертификата необходимо скопировать новый отпечаток сертификата в веб-интерфейсе и перезапустить сервис с обновленным значением параметра.

   - <agent_ID> — идентификатор сервиса агента, созданного в Kaspersky SIEM Cloud.
   - <user> — имя пользователя, под которым будет работать агент, включая домен.

5. При первой установке обновленного агента на устройстве требуется подтверждение лицензии. В процессе установки вам будет предложено ознакомиться с текстом лицензии и у вас будет возможность принять соглашение или отказаться. Если этого не произошло автоматически, вы можете воспользоваться следующей командой, чтобы ознакомиться с текстом лицензии:

   `kuma.exe license --show`

   Если вы хотите принять лицензионное соглашение, выполните команду и нажмите `y`:

```
kuma.exe license
```

Агент обновлен.

Передача в Kaspersky SIEM Cloud событий из изолированных сегментов сети

Схема передачи данных

С помощью диодов данных можно передавать события из изолированных сегментов сети в Kaspersky SIEM Cloud. Передача данных организована следующим образом:

1. Установленный на изолированном сервере агент Kaspersky SIEM Cloud с точкой назначения **diode** принимает события и перемещает их в директорию, из которой события заберет диод данных.

   Агент накапливает события в буфере до его переполнения или в течение заданного пользователем срока после последней записи на диск. Затем события записываются в файл во временной директории агента. Файл перемещается в директорию, обрабатываемую диодом данных; в качестве его названия используется хеш-сумма (SHA-256) содержимого файла и время создания файла.

2. Диод данных перемещает файлы из директории изолированного сервера в директорию внешнего сервера.

3. Установленный на внешнем сервере коллектор Kaspersky SIEM Cloud с коннектором **diode** считывает и обрабатывает события из файлов той директории, в которой размещает файлы диод данных.

   После считывания из файла всех событий он автоматически удаляется. Перед считыванием событий происходит верификация содержимого файлов по хеш-сумме в названии файла. Если содержимое не проходит верификацию, файл удаляется.

В указанной выше схеме компоненты Kaspersky SIEM Cloud отвечают за перемещение событий в определенную директорию внутри изолированного сегмента и за прием событий из определенной директории во внешнем сегменте сети. Перемещение файлов с событиями из директории изолированного сегмента сети в директорию внешнего сегменте сети осуществляет диод данных.

Для каждого источника данных внутри изолированного сегмента сети необходимо создать свой агент и коллектор Kaspersky SIEM Cloud, а также настроить диод данных на работу с отдельными директориями.

Настройка компонентов Kaspersky SIEM Cloud

Настройка компонентов Kaspersky SIEM Cloud для передачи данных из изолированных сегментов сети состоит из следующих этапов:

1. Создание сервиса коллектора во внешнем сегменте сети.

   На этом этапе необходимо создать и установить коллектор для получения и обработки файлов, которые диод данных будет перемещать из изолированного сегмента сети. Создать коллектор и все требуемые для него ресурсы можно с помощью мастера установки коллектора.

   На шаге **Транспорт** требуется выбрать или создать коннектор типа **diode**. В коннекторе необходимо указать директорию, в которую диод данных будет перемещать файлы из изолированного сегмента сети.

Пользователь kuma, под которым работает коллектор, должен иметь права на чтение, запись и удаление в директории, в которую диод данных перемещает данные из изолированного сегмента сети.

2. Создание набора ресурсов агента Kaspersky SIEM Cloud.

   На этом этапе необходимо создать набор ресурсов агента Kaspersky SIEM Cloud, который будет в изолированном сегменте сети получать события и подготавливать их для передачи диоду данных. Набор ресурсов diode-агента имеет следующие особенности:

   - Точка назначения в агенте должна иметь тип **diode**. В этом ресурсе необходимо указать директорию, из которой диод данных будет перемещать файлы во внешний сегмент сети.
   - Для diode-агента невозможно выбрать коннекторы типа **sql** или **netflow**.
   - В коннекторе diode-агента допускаются следующие значения параметра **Режим TLS**: **Выключено**, **Нестандартный PFX**, **Нестандартный PFX с аутентификацией клиента**. При выбранном значении **Включено** скачать конфигурационный файл невозможно.

3. Скачивание конфигурационного файла агента в виде JSON-файла.

   a. Набор ресурсов агента с точкой назначения типа diode необходимо скачать в виде JSON-файла.

   b. Если в наборе ресурсов агента использовались ресурсы секретов, конфигурационный файл необходимо вручную дополнить данными секретов.

4. Установка сервиса агента Kaspersky SIEM Cloud в изолированном сегменте сети.

   На этом этапе необходимо установить агент в изолированном сегменте сети на основе конфигурационного файла агента, созданного на предыдущем этапе. Установка возможна на устройствах Linux и Windows.

Настройка диода данных

Диод данных необходимо настроить следующим образом:

- Данные необходимо передавать атомарно из директории изолированного сервера (куда их помещает агент Kaspersky SIEM Cloud) в директорию внешнего сервера (где их считывает коллектор Kaspersky SIEM Cloud).
- Переданные файлы необходимо удалять с изолированного сервера.

Сведения о настройке диода данных можно получить в документации используемого в вашей организации диода данных.

Особенности работы

При работе с изолированными сегментами сети не поддерживаются работа с SQL и NetFlow.

При использовании указанной выше схемы невозможно администрирование агента через веб-интерфейс Kaspersky SIEM Cloud, поскольку он располагается в изолированном сегменте сети. В списке активных сервисов Kaspersky SIEM Cloud такие агенты не отображаются.

Конфигурационный файл diode-агента

Созданный набор ресурсов агента с точкой назначения типа **diode** можно скачать в виде конфигурационного файла. Этот файл используется при установке агента в изолированном сегменте сети.

Чтобы скачать конфигурационный файл,

1. В веб-консоли откройте раздел **Мониторинг** → **Ресурсы и сервисы** → **Агенты**.

2. Выберите нужный набор ресурсов агента с точкой назначения diode и нажмите **Скачать конфигурацию**.

Конфигурация параметров агента скачивается в виде JSON-файла в соответствии с параметрами вашего браузера. Секреты, использованные в наборе ресурсов агента, скачиваются пустыми, их идентификаторы указаны в файле в секции `secrets`. Для использования файла конфигурации для установки агента в изолированном сегменте сети необходимо вручную дополнить файл конфигурации секретами (например, указать URL и пароли, используемые в коннекторе агента для получения событий).

С помощью списка контроля доступа (ACL) нужно настроить права доступа к файлу на сервере, где будет установлен агент. Чтение файла должно быть доступно пользователю, от имени которого будет запускаться diode-агент.

Пример конфигурационного файла diode-агента с коннектором типа kafka

```
{
    "config": {
        "id": "<идентификатор набора ресурсов агента>",
        "name": "<название набора ресурсов агента>",
        "proxyConfigs": [
            {
                "connector": {
                    "id": "<идентификатор коннектора. В этом примере приводится коннектор типа kafka, но в diode-агенте можно использовать коннекторы и других типов. Если коннектор создан непосредственно в наборе ресурсов агента, значение идентификатора отсутствует.>",
                    "name": "<название коннектора>",
                    "kind": "kafka",
                    "connections": [
                        {
                            "kind": "kafka",
                            "urls": [
                                "localhost:9093"
                            ],
                            "host": "",
                            "port": "",
                            "secretID": "<идентификатор секрета>",
                            "clusterID": "",
                            "tlsMode": "",
                            "proxy": null,
                            "rps": 0,
                            "maxConns": 0,
                            "urlPolicy": "",
                            "version": "",
                            "identityColumn": "",
                            "identitySeed": "",
                            "pollInterval": 0,
                            "query": "",
                            "stateID": "",
                            "certificateSecretID": "",
                            "authMode": "pfx",
                            "secretTemplateKind": "",
                            "certSecretTemplateKind": ""
                        }
                    ],
                    "topic": "<название топика kafka>",
                    "groupID": "<идентификатор группы kafka>",
                    "delimiter": "",
                    "bufferSize": 0,
                    "characterEncoding": "",
```

```
                    "query": "",
                    "pollInterval": 0,
                    "workers": 0,
                    "compression": "",
                    "debug": false,
                    "logs": [],
                    "defaultSecretID": "",
                    "snmpParameters": [
                        {
                            "name": "",
                            "oid": "",
                            "key": ""
                        }
                    ],
                    "remoteLogs": null,
                    "defaultSecretTemplateKind": ""
                },
                "destinations": [
                    {
                        "id": "<идентификатор точки назначения. Если точка назначения создана непосредственно в
наборе ресурсов агента, значение идентификатора отсутствует.>",
                        "name": "<название точки назначения>",
                        "kind": "diode",
                        "connection": {
                            "kind": "file",
                            "urls": [
                                "<путь к директории, в которую точка назначения должна помещать события для
передачи из изолированного сегмента сети диодом данных>",
                                "<путь к временной директории, в которую помещаются события для подготовки к
передаче диодом данных>"
                            ],
                            "host": "",
                            "port": "",
                            "secretID": "",
                            "clusterID": "",
                            "tlsMode": "",
                            "proxy": null,
                            "rps": 0,
                            "maxConns": 0,
                            "urlPolicy": "",
                            "version": "",
                            "identityColumn": "",
                            "identitySeed": "",
                            "pollInterval": 0,
                            "query": "",
                            "stateID": "",
                            "certificateSecretID": "",
                            "authMode": "",
                            "secretTemplateKind": "",
                            "certSecretTemplateKind": ""
                        },
                        "topic": "",
                        "bufferSize": 0,
                        "flushInterval": 0,
                        "diskBufferDisabled": false,
                        "diskBufferSizeLimit": 0,
                        "healthCheckPath": "",
                        "healthCheckTimeout": 0,
                        "healthCheckDisabled": false,
                        "timeout": 0,
                        "workers": 0,
                        "delimiter": "",
                        "debug": false,
                        "disabled": false,
                        "compression": "",
                        "filter": null,
                        "path": ""
                    }
                ]
            }
        ],
        "workers": 0,
        "debug": false
    },
    "secrets": {
        "<идентификатор секрета>": {
            "pfx": "<зашифрованный pfx-ключ>",
            "pfxPassword": "<пароль к зашифрованному pfx-ключу. Вместо действительного пароля из Kaspersky SIEM
Cloud экспортируется значение changeit. В файле конфигурации необходимо вручную указать содержимое секретов>"
        }
    },
```

```
    "tenantID": "<идентификатор тенанта>"
}
```

Описание полей секретов

Поля секрета

Название поля	Тип	Описание
`user`	строка	Имя пользователя
`password`	строка	Пароль
`token`	строка	Токен
`urls`	массив строк	Список URL
`publicKey`	строка	Публичный ключ (используется в PKI)
`privateKey`	строка	Приватный ключ (используется в PKI)
`pfx`	строка, содержащая base64-закодированное содержимое pfx	Содержимое pfx-файла, закодированное в base64. На Linux получить base64-кодировку файла можно при помощи команды: `base64 -w0 src > dst`
`pfxPassword`	строка	Пароль от pfx
`securityLevel`	строка	Используется в snmp3. Возможные значения: `NoAuthNoPriv`, `AuthNoPriv`, `AuthPriv`
`community`	строка	Используется в snmp1
`authProtocol`	строка	Используется в snmp3. Возможные значения: `MD5`, `SHA`, `SHA224`, `SHA256`, `SHA384`, `SHA512`
`privacyProtocol`	строка	Используется в snmp3. Возможные значения: `DES`, `AES`
`privacyPassword`	строка	Используется в snmp3
`certificate`	строка, содержащая base64-закодированное содержимое pem	Содержимое pem-файла, закодированное в base64. На Linux получить base64-кодировку файла можно при помощи команды: `base64 -w0 src > dst`

Установка Linux-агента в изолированном сегменте сети

Чтобы установить в изолированном сегменте сети агент Kaspersky SIEM Cloud на устройство Linux:

1. Поместите на Linux-сервер в изолированном сегменте сети, который будет использоваться для получения агентом событий и с которого диод данных будет перемещать файлы во внешний сегмент сети, следующие файлы:

   - Конфигурационный файл агента.

     Необходимо при помощи списка контроля доступа (ACL) настроить права доступа к конфигурационному файлу так, чтобы доступ на чтение файла был только у пользователя KUMA.

   - Исполняемый файл /opt/kaspersky/kuma/agent (файл `agent` можно найти внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/).

2. Выполните следующую команду:

```
sudo ./agent agent --cfg <config_path> --wd <directory_path>
```

где:

- <config_path> — путь к конфигурационному файлу агента.
- <directory_path> — путь к директории, где будут размещаться файлы устанавливаемого агента. Если не указывать этот флаг, файлы будут храниться в директории, где расположен файл `agent`.

3. Если вы хотите принять Лицензионное соглашение, введите `y`, когда установщик запросит подтверждение принятия соглашения. Запуск агента невозможен без принятия Лицензионного соглашения.

4. Введите пароль для конфигурационного файла агента, заданный при скачивании конфигурационного файла.

Сервис агента установлен и запущен на сервере в изолированном сегменте сети. Он получает события и передает их диоду данных для отправки во внешний сегмент сети.

Установка Windows-агента в изолированном сегменте сети

Перед установкой агента Kaspersky SIEM Cloud на устройстве Windows администратору сервера необходимо создать на устройстве Windows учетную запись с правами EventLogReaders и Log on as a service. Эту же учетную запись необходимо использовать для запуска агента.

Чтобы установить в изолированном сегменте сети агент Kaspersky SIEM Cloud на устройство Windows:

1. Поместите на Window-сервер в изолированном сегменте сети, который будет использоваться для получения агентом событий и с которого диод данных будет перемещать файлы во внешний сегмент сети, следующие файлы:

   - Конфигурационный файл агента.

     Необходимо при помощи списка контроля доступа (ACL) настроить права доступа к конфигурационному файлу так, чтобы доступ на чтение файла был только у пользователя, под которым будет работать агент.

   - Исполняемый файл kuma.exe. Файл можно найти внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

   Рекомендуется использовать папку `C:\Users\<имя пользователя>\Desktop\KUMA`.

2. Запустите командную строку на устройстве Windows с правами администратора и найдите папку с файлом kuma.exe.

3. Выполните следующую команду:

```
kuma.exe agent --cfg <config_path> --user <user_name> --install
```

Где:

- <config_path> — путь к конфигурационному файлу агента.
- <user_name> — имя пользователя, под которым будет работать агент, включая домен.

Справочная информация об установщике доступна по команде:

```
kuma.exe help agent
```

4. Чтобы автоматически принять Лицензионное соглашение во время установки, добавьте параметр `--accept-eula`. Без этого параметра установщик запросит подтверждение принятия соглашения.

   Примеры команд:

   - Установка с интерактивным принятием Лицензионного соглашения:

     ```
     sudo ./agent agent --cfg <config_path> --user <user_name> --install
     ```

   - Установка с автоматическим принятием Лицензионного соглашения:

     ```
     sudo ./agent agent --cfg <config_path> --user <user_name> --accept-eula --install
     ```

   Чтобы просмотреть текст Лицензионного соглашения после установки, выполните команду:

   ```
   ./agent license --show
   ```

5. Введите пароль для конфигурационного файла агента, заданный при скачивании конфигурационного файла.

6. Введите пароль для пользователя, под которым будет работать агент.

Создана папка `C:\Program Files\Kaspersky Lab\KUMA\agent\<идентификатор агента>`, в нее установлен сервис агента Kaspersky SIEM Cloud. Агент перемещает события в папку для обработки диодом данных.

При установке агента конфигурационный файл агента перемещается в директорию C:\Program Files\Kaspersky Lab\KUMA\agent\<идентификатор агента, указанный в конфигурационном файле>. Файл kuma.exe перемещается в директорию C:\Program Files\Kaspersky Lab\KUMA.

При установке агента его конфигурационный файл не должен находиться в директории, в которую устанавливается агент.

Когда сервис агента установлен, он запускается автоматически. Сервис также настроен на перезапуск в случае сбоев.

Удаление агента Kaspersky SIEM Cloud с устройств Windows

Чтобы удалить агент Kaspersky SIEM Cloud с устройства Windows:

1. Запустите командную строку на компьютере Windows с правами администратора и найдите папку с файлом kuma.exe.

2. Выполните любую из команд ниже:

   - `kuma.exe agent --cfg <путь к файлу конфигурации агента> --uninstall`

   - `kuma.exe agent --id <идентификатор сервиса агента, созданного в Kaspersky SIEM Cloud> --uninstall`

Указанный агент Kaspersky SIEM Cloud удален с устройства Windows. События Windows больше не отправляются в Kaspersky SIEM Cloud.

При настройке сервисов можно проверить конфигурацию на наличие ошибок до установки, запустив агент с помощью команды:

```
kuma.exe agent --cfg <путь к конфигурационному файлу агента>
```

Настройка агента для получения событий Netflow из изолированного сегмента сети

Для приема событий Netflow из изолированного сетевого сегмента используется выделенный агент, установленный внутри этого сегмента. Агент выполняет роль промежуточного узла: он принимает события NetFlow локально и пересылает их в коллектор, где настроен коннектор Netflow.

Передача событий от агента коллектору осуществляется по протоколу UDP.

Чтобы настроить получение событий netflow:

1. Создайте или настройте коллектор с коннектором netflow и на шаге **Транспорт** на вкладке **Дополнительные параметры** укажите для параметра **Размер буфера** значение **65467**.

2. Убедитесь, что изолированный сегмент разрешает исходящий UDP-трафик к коллектору.

3. Создайте агент для получения событий и настройте передачу событий в коллектор с коннектором **netflow**:

   a. В главном меню OSMP в разделе **Ресурсы и сервисы** → **Агенты** нажмите **Создать**.

   b. В открывшемся окне **Создание агента** на вкладке **Общие параметры** задайте параметры **Название** и **Тенант**.

c. На вкладке **Подключение №{{index}}** в блоке **Коннектор** на вкладке **Основные параметры** укажите следующие параметры:

- **Название** – укажите название коннектора.
- **Тип** – укажите тип коннектора **udp**.
- **URL** – укажите устройство, на котором будет установлен агент для получения событий Netflow.

d. На вкладке **Подключение №{{index}}** в блоке **Коннектор** на вкладке **Дополнительные параметры** укажите следующие параметры:

- **Размер буфера** – укажите значение **65467**. Это максимальный размер буфера в байтах.

e. На вкладке **Подключение №{{index}}** в блоке **Точки назначения** на вкладке **Основные параметры** укажите следующие параметры:

- **Название** – укажите название точки назначения.
- **Тип** – укажите протокол UDP, по которому будет выполняться передача событий.
- **URL** – укажите устройство, на котором установлен коллектор с коннектором **netflow**.

f. На вкладке **Подключение №{{index}}** в блоке **Точки назначения** на вкладке **Дополнительные параметры** укажите следующие параметры:

- **Размер буфера** – укажите значение **65467**. Это максимальный размер буфера в байтах.

g. Нажмите **Создать**.

h. Установите агент в изолированном сегменте сети. Установка возможна на устройствах Linux и Windows.

Настройка получения событий Netflow из изолированного сегмента завершена.

Получение служебных данных о событиях из изолированного сегмента

Служебные данные о событиях передаются в коллектор по протоколу internal. Для передачи таких данных из изолированного сетевого сегмента используется выделенный агент, установленный внутри этого сегмента.

Для передачи данных от агента в коллектор по протоколу internal между агентом и коллектором должна произойти взаимная аутентификация с помощью сертификатов. Вы можете создать и сохранить сертификат агента в конфигурационный файл агента и затем использовать этот файл для установки агента в изолированном сегменте. Данные о сертификате сохраняются в файле в зашифрованном виде.

Чтобы настроить получение служебных данных о событиях из изолированного сегмента:

1. Создайте или настройте коллектор с коннектором internal.
2. Создайте агент и настройте передачу данных в коллектор:
   a. В веб-консоли в разделе **Мониторинг** → **Ресурсы и сервисы** → **Агенты** нажмите **Создать**.
   b. В открывшемся окне **Создание агента** на вкладке **Общие параметры** задайте параметры **Название** и **Тенант**.
   c. На вкладке **Подключение №{{index}}** в блоке **Коннектор** укажите следующие параметры:
      - **Название** – укажите название коннектора.
      - **Тип** – укажите тип коннектора.
      - **URL** – укажите хост, на котором будет установлен агент для получения событий.
   d. На вкладке **Подключение №{{index}}** в блоке **Точки назначения** укажите следующие параметры:
      - **Название** – укажите название точки назначения.
      - **Тип** – укажите протокол **internal**, по которому будет выполняться передача событий.
      - **URL** – укажите хост, на котором установлен коллектор с коннектором **internal**.
   e. Нажмите **Создать**.
   f. Выберите из списка созданный набор ресурсов агента и затем в окне свойств агента нажмите **Скачать конфигурацию, содержащую сертификат**. В открывшемся окне задайте пароль, который будет использован для шифрования сертификата, а также будет запрашиваться при запуске агента.

      Конфигурация параметров агента скачивается в виде JSON-файла в соответствии с параметрами вашего браузера. Этот файл используется при установке агента в изолированном сегменте сети.

      > Необходимо при помощи списка контроля доступа (ACL) настроить права доступа к файлу на сервере, где будет установлен агент. Чтение файла должно быть доступно пользователю, от имени которого будет запускаться агент.

   g. Установите агент в изолированном сегменте сети. Установка возможна на устройствах Linux и Windows.

Настройка получения служебных данных о событиях из изолированного сегмента завершена.

Получение чувствительных данных по защищенному соединению

Источники событий передают данные по сети без шифрования. Если данные содержат чувствительную информацию, передача таких данных по сети в открытом виде недопустима.

В OSMP можно использовать агент для передачи данных от источника в коллектор по защищенному соединению. При этом способ передачи данных от источника к агенту зависит от того, где установлен агент.

Доступны следующие способы:

- Получение данных по протоколу internal.

  Агент Kaspersky SIEM Cloud устанавливается на том же хосте, что и источник событий. Источник событий передает данные агенту локально в виде файла, а агент передает их в коллектор по протоколу internal.

- Получение данных по протоколу с поддержкой TLS-шифрования.

  Агент Kaspersky SIEM Cloud устанавливается в изолированном сегменте сети, не обязательно на хосте с источником событий. Источник событий передает данные агенту по UDP в виде пакетов данных, а агент передает полученные данные в коллектор по протоколу с поддержкой TLS-шифрования. В этом случае незашифрованная передача по UDP ограничена изолированным сегментом сети, а передача от агента к коллектору выполняется с шифрованием.

Получение данных по протоколу internal

Ниже приведен пример настройки получения данных, в котором агент Kaspersky SIEM Cloud установлен на хосте с источником. Агент получает события от источника и передает их в коллектор в виде файла по внутреннему протоколу internal. Вы можете адаптировать этот пример в соответствии со своими потребностями.

Чтобы настроить получение событий по протоколу internal:

1. Создайте или настройте коллектор и на шаге **Транспорт** на вкладке **Дополнительные параметры** укажите для параметра **Размер буфера** значение **65467**.

2. Создайте агент для получения событий и настройте передачу событий в коллектор по протоколу internal:

   a. В веб-консоли в разделе **Мониторинг** → **Ресурсы и сервисы** → **Агенты** нажмите **Создать**.

   b. В открывшемся окне **Создание агента** на вкладке **Общие параметры** задайте параметры **Название** и **Тенант**.

   c. Откройте вкладку **Подключение №{{index}}**.

   d. В блоке **Коннектор** укажите следующие параметры:

      1. На вкладке **Основные параметры**:

         - **Название** – укажите название коннектора.
         - **Тип** – укажите тип **file**.
         - **Путь к файлу** – укажите полный путь к файлу с журналами.

      2. На вкладке **Дополнительные параметры** в поле **Размер буфера** укажите значение **65467**.

         Это максимальный размер буфера в байтах.

e. В блоке **Точки назначения** укажите следующие параметры:

1. На вкладке **Основные параметры**:

   - **Название** – укажите название точки назначения.
   - **Тип** – укажите протокол **internal**, по которому будет выполняться передача событий.
   - **URL** – укажите хост, на котором установлен коллектор для получения данных.

2. На вкладке **Дополнительные параметры** в поле **Размер буфера** укажите значение **65467**.

   Это максимальный размер буфера в байтах.

f. Нажмите **Создать**.

g. Установите агент на хосте с источником событий. Установка возможна на устройствах Linux и Windows.

Настройка получения событий по протоколу internal завершена.

Получение данных по протоколу с поддержкой TLS-шифрования

Ниже приведен пример настройки получения данных, в котором агент Kaspersky SIEM Cloud установлен на отдельном хосте, не обязательно на хосте с источником событий. Агент получает данные от источника событий в изолированном сегменте и передает их в коллектор по протоколу с поддержкой TLS-шифрования. Вы можете адаптировать этот пример в соответствии со своими потребностями.

Чтобы настроить получение данные по протоколу с поддержкой TLS-шифрования:

1. Создайте или настройте коллектор и на шаге **Транспорт** на вкладке **Дополнительные параметры** укажите для параметра **Размер буфера** значение **65467**.

2. Создайте агент для получения событий и настройте передачу событий в коллектор по протоколу, поддерживающему TLS-шифрование:

   a. В веб-консоли в разделе **Мониторинг** → **Ресурсы и сервисы** → **Агенты** нажмите **Создать**.

   b. В открывшемся окне **Создание агента** на вкладке **Общие параметры** задайте параметры **Название** и **Тенант**.

   c. Откройте вкладку **Подключение №{{index}}**.

   d. В блоке **Коннектор** укажите следующие параметры:

      1. На вкладке **Основные параметры**:

         - **Название** – укажите название коннектора.
         - **Тип** – укажите тип **udp**.
         - **URL** – укажите хост, на котором будет установлен агент для получения событий.

2. На вкладке **Дополнительные параметры** в поле **Размер буфера** укажите значение **65467**.

   Это максимальный размер буфера в байтах.

e. В блоке **Точки назначения** укажите следующие параметры:

1. На вкладке **Основные параметры**:

   - **Название** – укажите название точки назначения.
   - **Тип** – укажите протокол, по которому будет выполняться передача событий. Вы можете указать любой протокол, поддерживающий TLS-шифрование.
   - **URL** – укажите хост, на котором установлен коллектор.

2. На вкладке **Дополнительные параметры**:

   - **Размер буфера** – укажите значение **65467**. Это максимальный размер буфера в байтах.
   - **Режим TLS** – в раскрывающемся списке выберите значение **Включено**.

f. Нажмите **Создать**.

g. Установите агент в изолированном сегменте сети. Установка возможна на устройствах Linux и Windows.

Настройка получения событий по протоколу, поддерживающему TLS-шифрование, завершена.

Передача в OSMP событий с машин Windows

Для передачи событий с машин Windows в OSMP используются агент и коллектор Kaspersky SIEM Cloud. Передача данных выполняется следующим образом:

1. Установленный на машине агент Kaspersky SIEM Cloud получает события Windows с помощью одного из коннекторов:

   - WEC. Агент получает события, поступающие на хост по подписке (subscription), и журналы сервера.
   - WMI. Агент подключается к удаленным серверам, указанным в конфигурации, и получает события.
   - ETW. Агент использует для подключения к DNS-серверу имя сессии и провайдера, указанные в параметрах коннектора, и получает события.

2. Агент без предварительной обработки передает события коллектору Kaspersky SIEM Cloud, указанному в точке назначения.

   Можно настроить агент таким образом, чтобы разные журналы отправлялись в разные коллекторы.

3. Коллектор принимает события от агента, выполняет полный цикл обработки события и отправляет обработанные события в точку назначения.

Об использовании агентов

Настроить получение событий с устройств Windows с помощью Агента KUMA (WEC) рекомендуется при использовании централизованного получения событий с хостов Windows с помощью технологии Windows Event Forwarding (WEF) (подробнее о Windows Event Forwarding см. в официальной документации Microsoft). Агент нужно установить на сервер, который выполняет сбор событий и который будет выполнять функции Windows Event Collector (WEC). Мы не рекомендуем устанавливать агенты Kaspersky SIEM Cloud на каждый конечный хост, с которого планируется получать события.

Настроить получение событий с помощью агента Агента Kaspersky SIEM Cloud (WMI) рекомендуется в следующих случаях:

- Отсутствует возможность использовать технологию WEF для реализации централизованного сбора событий, а также на сервере-источнике событий (например, агент Kaspersky SIEM Cloud) запрещено устанавливать стороннее программное обеспечение.
- Требуется выполнить сбор событий с небольшого количества хостов (не более 500 хостов для одного агента Kaspersky SIEM Cloud).

Агент ETW используется только для получения событий из журналов Windows DNS-серверов.

Для подключения журналов Windows в качестве источника событий рекомендуется использовать мастер **Подключить источник**. При использовании мастера в процессе создания коллектора с коннекторами типами WEC и WMI автоматически создаются агенты для приема событий Windows. Также ресурсы, необходимые для сбора событий Windows, можно создать вручную.

Создание и установка агента и коллектора Kaspersky SIEM Cloud

Создание и установка агента и коллектора для получения событий Windows состоит из следующих этапов:

1. **Создание набора ресурсов агента**

   Коннектор агента:

   При создании агента на вкладке **Подключение** создайте или выберите коннектор типа WEC, WMI или ETW.

   Если хотя бы одно название журнала Windows указано в коннекторе типа WEC или WMI с ошибкой или сервер WMI недоступен, агент будет получать события из всех перечисленных в коннекторе журналов Windows, кроме проблемного. При этом статус агента будет зеленый. Попытки получить события будут повторяться каждые 60 секунд, сообщения об ошибке будут добавляться в журнал сервиса.

   Точка назначения агента:

   Тип точки назначения агента зависит от используемого вами способа передачи данных: `nats-jetstream`, `tcp`, `http`, `diode`, `kafka`, `file`.

   В качестве разделителя в точке назначения используйте значение `\0`.

   Дополнительные параметры точки назначения агента (например, разделитель, сжатие и режим TLS) должны совпадать с дополнительными параметрами коннектора коллектора, с которым вы связываете агент.

2. **Создание сервиса агента в веб-интерфейсе Kaspersky SIEM Cloud**

3. **Установка агента Kaspersky SIEM Cloud на машине Windows, с которой вы хотите получать события Windows**

   Перед установкой убедитесь, что компоненты системы имеют доступ к сети и откройте необходимые сетевые порты:

   - Порт 7210, протокол TCP – от сервера с коллекторами к Ядру.
   - Порт 7210, протокол TCP – от сервера агента к Ядру.
   - Порт, указанный при создании коннектора в поле **URL** – от сервера агента к серверу с коллектором.

4. **Создание и установка коллектора Kaspersky SIEM Cloud**

   При создании набора ресурсов коллектора на шаге **Транспорт** создайте или выберите существующий коннектор, с помощью которого коллектор будет получать события от агента. Тип коннектора должен совпадать с типом точки назначения агента.

   Дополнительные параметры коннектора, такие как разделитель, сжатие и режим TLS, должны совпадать с дополнительными параметрами точки назначения агента, с которой вы хотите связать агент.

Полезные статьи

Ошибка Access is denied

События не поступают через WMI-агент

Импорт файла со списком серверов для агентов WMI

Вы можете импортировать файл в формате .TSV со списком источников событий для агентов WMI, чтобы не заполнять вручную параметры **Сервер**, **Домен** и **Тип журналов** для агента WMI каждого сервера, когда таких серверов много. В таком файле вы можете подготовить список серверов, к которым будет подключаться агент WMI, и список журналов, которые вы хотите получать от указанных серверов.

Требования к файлу со списком серверов для агентов WMI

Допустимый формат файла: TSV.

Если вы поменяете рекомендуемый формат на **All files** и загрузите файл, не соответствующий требуемому формату (например, вместо TSV загружен файл JSON, XML или в другом формате), парсинг такого файла может быть выполнен некорректно.

Максимальное количество строк в файле с параметрами хостов: 500.

Следующие поля являются обязательными для заполнения:

- **Сервер** – имя хоста, от которого агент будет получать журналы. Допустимый формат: имя хоста или IP-адрес. Допустимые значения: IPv4, IPv6, имя хоста.
- **Домен** – идентификатор хоста, по которому будет выполняться обращение к хосту по сети. Допустимый формат: полное доменное имя или IP-адрес. Допустимые значения: IPv4, IPv6, FQDN.

- **Тип журналов** – список журналов и/или подписок Windows, которые будет получать агент. Допустимый формат: массив строк. Например, вы можете указать значение Application, ForwardedEvents или Security. Если в файле указано значение, ранее отсутствовавшее в списке журналов, должны быть созданы пользовательский журнал или подписка, которые также появятся в списке доступных к обработке с помощью Windows-агента.

  Допустимо указать значение журнала, которое имеет максимальную длину – 1024 символа. Должно быть указано не менее одного журнала или подписки.

После импорта и заполнения всех полей удаленных хостов при сохранении параметров выполняется проверка. Если в полях допущены ошибки, параметры не сохранятся, а допущенные ошибки будут выделены. Вы можете вручную внести необходимые правки в полях и сохранить параметры.

Чтобы импортировать файл со списком источников:

1. В веб-консоли в разделе **Мониторинг** → **Ресурсы и сервисы** → **Агенты** создайте агент WMI или откройте параметры агента WMI для редактирования.

2. В открывшемся окне на вкладке **Подключение №** в блоке параметров **Коннектор** укажите название коннектора, в раскрывающемся списке **Тип** выберите **wmi** и нажмите на кнопку **Импортировать TSV**.

3. В открывшемся окне выберите подготовленный файл со списком источников в формате .TSV.

   OSMP выполняет парсинг файла и в блоке параметров **Удаленные хосты** заполняет данными обязательные поля **Сервер**, **Домен**, **Тип журналов**.

4. При необходимости в раскрывающемся списке **Секрет** выберите секрет с типом **Credentials** либо создайте секрет с типом **Credentials**.

   При импорте списка хостов из файла, в раскрывающемся списке **Секрет** остается значение **По умолчанию** и агент будет применять учетные данные по умолчанию при обращении к серверу для получения журналов.

5. Если вы хотите отменить импорт данных из файла, нажмите **Отмена**. Если вы хотите убрать некоторые строки с данными, импортированными из файла, в интерфейсе выделите необходимые для удаления строки и нажмите **Удалить**.

6. Сохраните параметры, выполнив одно из следующих действий:

   - Для созданного агента нажмите **Создать**. Сервис будет создан в веб-консоли.

   - Для действующего агента, открытого для редактирования, нажмите **Сохранить**.

7. Примените сохраненные параметры, выполнив одно из следующих действий:

   - Для созданного агента установите сервис агента в сетевой инфраструктуре OSMP.

   - Для действующего сервиса агента, открытого для редактирования, перезапустите сервис агента.

Файл со списком серверов для агентов WMI будет импортирован.

Хранение конфиденциальной информации (секреты)

Для безопасного хранения конфиденциальной информации, такой как логины и пароли, которые Kaspersky SIEM Cloud использует для взаимодействия с внешними службами, используются *секреты*. Если секрет хранит данные учетной записи, такие как логин и пароль, то при подключении коллектора к источнику событий учетная запись, заданная в секрете, может быть заблокирована согласно настроенной в системе-источнике событий парольной политике.

Секреты можно использовать в коллекторах и коннекторах при использовании шифрования TLS, точках назначения при использовании шифрования TLS или авторизации, а также для прокси-серверов.

Просмотр секретов

Чтобы просмотреть секреты,

в веб-консоли откройте раздел **Мониторинг** → **Ресурсы и сервисы** → **Секреты**.

Откроется таблица секретов.

Секрет, созданный внутри ресурса в тенанте Shared, не отображается в разделе **Мониторинг** → **Ресурсы и сервисы** → **Секреты** и недоступен для просмотра, в том числе пользователю с ролью Главный администратор. Такой секрет доступен для просмотра и действий внутри ресурса, в котором создан, и доступен только для просмотра в разделе **Мониторинг** → **Ресурсы и сервисы** при выбранном типе отображения **Список**.

Секреты можно искать по названию с помощью поля **Поиск**. При поиске секретов используются регулярные выражения.

Таблицу можно сортировать по названию, типу, времени последнего обновления и по названию пакета, нажав на значок сортировки ⌄ в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

Таблица секретов содержит следующие столбцы:

- **Имя** – название секрета.
- **Тип** – тип секрета. Вы можете искать типы, нажав на значок сортировки в заголовке столбца, указав значение для поиска в поле **Поиск** или выбрав типы с помощью флажков.
- **Путь до ресурса** – тенант, которому принадлежит секрет.
- **Последнее обновление** – дата и время последнего обновления секрета.
- **Создал** – имя пользователя, создавшего секрет.
- **Описание** – информация о секрете, которую вы можете добавить при необходимости.

- **Теги** – теги для поиска секрета. Вы можете искать секреты по тегам, нажав на значок сортировки в заголовке столбца, указав значение для поиска в поле **Поиск** или выбрав теги с помощью флажков.
- **Названия пакетов** – название пакета инструментов, предназначенного для обработки событий.

Создание секрета

Чтобы создать секрет:

1. В веб-консоли откройте раздел **Мониторинг → Ресурсы и сервисы → Секреты**.
2. В панели инструментов или в меню ⋮ нажмите на кнопку **Создать**.
3. В открывшейся боковой панели в поле **Имя** введите уникальное имя секрета. Название должно содержать от 1 до 128 символов в кодировке Unicode.
4. В раскрывающемся списке **Тенант** выберите, к какому тенанту относится этот секрет.
5. В раскрывающемся списке **Тип** выберите тип правила обогащения и настройте параметры, специфичные для выбранного типа секрета:

   credentials

   Секрет типа **credentials** используется для хранения данных учетных записей, с помощью которых осуществляется подключение к таким внешним службам, как SMTP-серверы или СУБД. Например, когда секрет типа **credentials** используется для подключения коллектора к источнику событий, учетная запись, заданная в секрете, будет заблокирована при нарушении парольной политики, настроенной для источника событий.

   При выборе этого типа секрета заполните поля **Пользователь** и **Пароль**.

   При изменении ранее сохраненного секрета типа credentials поля с именем пользователя и паролем отображаются пустыми. Значения этих полей сохранены, вам не нужно вводить их повторно.

   token

   Секрет типа **token** используется, чтобы хранить токены для API-запросов. Токены используются, например, при подключении к IRP-системам.

   При выборе этого типа секрета заполните поле **Токен**.

   ktl

   Секрет типа **ktl** используется для хранения данных учетной записи Kaspersky Threat Intelligence Portal.

   При выборе этого типа секрета выполните следующие действия:

   1. В полях **Пользователь** и **Пароль** укажите имя пользователя и пароль вашей учетной записи Kaspersky Threat Intelligence Portal.
   2. По кнопке **Файл обмена личной информацией - PKCS (.PFX)** загрузите ключ сертификата Kaspersky Threat Intelligence Portal.
   3. В поле **Пароль PFX-файла** укажите пароль для доступа к ключу сертификата Kaspersky Threat Intelligence Portal.

urls

Секрет типа **urls** используется для хранения URL для подключения к базам SQL и прокси-серверам.

При выборе этого типа секрета заполните поле **URL**. Вы можете указать URL в форматах hostname:port, IPv4:port, IPv6:port, :port.

В поле **Описание** рекомендуется описать, для какого именно подключения вы используете секрет **urls**.

pfx

Секрет типа **pfx** используется для импорта PFX-файла с сертификатами.

При выборе этого типа секрета выполните следующие действия:

1. По кнопке **Файл обмена личной информацией - PKCS (.PFX)** загрузите PFX-файл.

   Файл должен содержать сертификат и ключ. В PFX-файлы можно включать сертификаты, подписанные центрами сертификации, для проверки сертификатов сервера.

   > Сертификат, включенный в PFX-файл, не может быть зашифрован алгоритмом AES-128-CBC. Kaspersky SIEM не поддерживает такие сертификаты.

2. В поле **Пароль PFX-файла** укажите пароль для доступа к ключу сертификата.

kata/edr

Секрет типа **kata/edr** используется для хранения файла сертификата и закрытого ключа, требуемых при подключении к серверу Kaspersky Endpoint Detection and Response.

При выборе этого типа секрета в блоке **Файлы аутентификации** выполните следующие действия:

1. При необходимости сгенерируйте сертификат и закрытый ключ шифрования.
2. Нажмите на кнопку **Загрузить сертификат** и загрузите сертификат сервера Kaspersky SIEM Cloud.

   Файл должен иметь формат PEM. Вы можете загрузить только один файл сертификата.
3. Нажмите на кнопку **Загрузить закрытый ключ** и загрузите файл RSA-ключа сервера Kaspersky SIEM Cloud.

   Ключ должен быть без пароля и с заголовком PRIVATE KEY. Вы можете загрузить только один файл ключа.

snmpV1/V2

Секрет типа **snmpV1/V2** используется для хранения значения **Уровень доступа** (например, `public` или `private`), которое требуется при взаимодействии по протоколу Simple Network Management Protocol.

При выборе этого типа секрета заполните поле **Уровень доступа**.

snmpV3

Секрет типа **snmpV3** используется для хранения данных, необходимых при взаимодействии по протоколу Simple Network Management Protocol.

При выборе этого типа секрета выполните следующие действия:

1. В поле **Пользователь** укажите имя пользователя без домена.
2. В раскрывающемся списке **Уровень безопасности** выберите один из следующих вариантов:
   - **NoAuthNoPriv** – сообщения отправляются без аутентификации и обеспечения конфиденциальности.
   - **AuthNoPriv** – сообщения отправляются с аутентификацией, но без обеспечения конфиденциальности.
   - **AuthPriv** – сообщения отправляются с аутентификацией и обеспечением конфиденциальности.
3. Если вы выбрали вариант **AuthNoPriv** или **AuthPriv**, в поле **Пароль** укажите пароль аутентификации пользователя SNMP.
4. Если вы выбрали вариант **AuthNoPriv** или **AuthPriv**, в раскрывающемся списке **Протокол аутентификации** выберите необходимый протокол: MD5, SHA, SHA224, SHA256, SHA384, SHA512.
5. Если вы выбрали вариант **AuthPriv**, в раскрывающемся списке **Протокол шифрования** выберите необходимый протокол: DES или AES
6. Если вы выбрали вариант **AuthPriv**, в поле **Пароль обеспечения безопасности** укажите пароль шифрования, который был указан при создании пользователя SNMP.

certificate

Секрет типа **certificate** используется для хранения файлов сертификатов.

При выборе этого типа секрета загрузите сертификат по кнопке **Загрузить файл сертификата**. Поддерживаются открытые ключи сертификата X.509 в Base64

fingerprint

Секрет типа **fingerprint** используется для хранения значения параметра **Elastic fingerprint**, которое может использоваться при подключении к серверу Elasticsearch.

При выборе этого типа сертификата заполните поле **Elastic fingerprint**.

private and public key

Секрет типа **public and private key** используется для подключения коллектора к ClickHouse.

При выборе этого варианта требуется указать секрет, содержащий закрытый ключ PEM, закодированный в base64, и открытый ключ.

ssh private key

Секрет типа **ssh private key** используется в коннекторе SFTP для подключения к SFTP-серверу.

При выборе этого варианта требуется указать имя пользователя и файл, содержащий закрытый SSH-ключ.

s3

Секрет типа **s3** используется для настройки хранилища S3.

При выборе этого варианта требуется указать имя ключа доступа и сам секретный ключ доступа.

6. При необходимости в раскрывающемся списке **Теги** выберите теги для секрета.

7. При необходимости в поле **Описание** добавьте описание секрета. Описание может содержать до 4000 символов в кодировке Unicode.

8. Нажмите на кнопку **Создать**.

Секрет будет сохранен и отобразится в таблице.

Удаление секрета

Чтобы удалить секрет:

1. В веб-консоли откройте раздел **Мониторинг → Ресурсы и сервисы** и выберите тип отображения ресурсов и сервисов **Список**.

   В режиме **Список** отображаются все секреты, включая встроенные секреты, созданные в ресурсах тенанта Shared. Такие секреты не отображаются в разделе **Секреты**.

2. Если секрет привязан к ресурсу, перед удалением отвяжите его одним из следующих способов:

   - В ресурсе выберите другой секрет. В этом случае текущий секрет будет автоматически отвязан и доступен для удаления.

   - Удалите ресурс, к которому привязан секрет. В этом случае секрет также будет автоматически отвязан и доступен для удаления.

3. В списке установите флажок рядом с секретом, который требуется удалить, и на панели инструментов нажмите **Удалить**.

Секрет удален.

Предустановленные секреты

В поставку Kaspersky SIEM Cloud входят перечисленные в таблице ниже секреты.

Предустановленные секреты

Название секрета	Описание
[OOTB] Continent SQL connection	Хранит конфиденциальные данные и параметры подключения к базе данных системы АПКШ Континент. Для использования необходимо указать логин и пароль базы данных.
\9210157[OOTB] InfoWatch Person Monitor MS SQL connection	Хранит конфиденциальные данные и параметры подключения к базе данных MS SQL системы InfoWatch Person Monitor. Для использования необходимо указать логин и пароль базы данных.
[OOTB] InfoWatch Traffic Monitor SQL Connection	Хранит конфиденциальные данные и параметры подключения к базе данных системы InfoWatch Traffic Monitor. Для использования необходимо указать логин и пароль базы данных.
[OOTB] Kaspersky Security for Exchange SQL connection	Хранит конфиденциальные данные и параметры подключения к базе данных системы Kaspersky Security для Microsoft Exchange Servers. Для использования необходимо указать логин и пароль базы данных.
[OOTB] KSC MSSQL connection	Хранит конфиденциальные данные и параметры подключения к базе данных MS SQL системы Open Single Management Platform. Для использования необходимо указать логин и пароль базы данных.
[OOTB] KSC MySQL Connection	Хранит конфиденциальные данные и параметры подключения к базе данных MySQL системы Open Single Management Platform. Для использования необходимо указать логин и пароль базы данных.

Название секрета	Описание
\9210157[OOTB] KSC PostgreSQL connection	Хранит конфиденциальные данные и параметры подключения к базе данных PostgreSQL системы Open Single Management Platform. Для использования необходимо указать логин и пароль базы данных.
[OOTB] Oracle Audit Trail SQL Connection	Хранит конфиденциальные данные и параметры подключения к базе данных системы Oracle. Для использования необходимо указать логин и пароль базы данных.
\9210157[OOTB] Parsec MSSQL connection	Хранит конфиденциальные данные и параметры подключения к базе данных MSSQL системы Parsec. Для использования необходимо указать логин и пароль базы данных.
[OOTB] SecretNet SQL connection	Хранит конфиденциальные данные и параметры подключения к базе данных MS SQL системы SecretNet. Для использования необходимо указать логин и пароль базы данных.
\9210157[OOTB] TeamPass MySQL connection	Хранит конфиденциальные данные и параметры подключения к базе данных MySQL системы TeamPass. Для использования необходимо указать логин и пароль базы данных.
[OOTB] Zabbix audit MySQL	Хранит конфиденциальные данные и параметры подключения к базе данных MySQL системы Zabbix. Для использования необходимо указать логин и пароль базы данных.

Работа с базой знаний

Для более наглядной работы с пакетами и ресурсами, которые поставляет "Лаборатория Касперского", в Kaspersky SIEM Cloud доступен раздел **База знаний.** В этом разделе можно просматривать доступные и установленные пакеты и ресурсы, устанавливать отдельные ресурсы или пакеты целиком, оценивать покрытие техник MITRE ATT&CK установленными ресурсами, отслеживать актуальность версий ресурсов, выполнять поиск и фильтрацию по заданным параметрам.

Пакеты содержат наборы ресурсов, предназначенных для настройки Kaspersky SIEM Cloud. Пакеты загружаются из репозитория "Лаборатории Касперского".

Если пакеты из репозитория еще не были загружены, в разделе **База знаний** список пакетов и ресурсов будет пустым. Чтобы получить доступные для установки пакеты и ресурсы, необходимо настроить обновление предустановленных ресурсов.

Просмотр информации о пакетах и ресурсах

Чтобы открыть базу знаний,

в веб-консоли перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **База знаний**.

Раздел содержит виджеты, отображающие сводную информацию о пакетах и ресурсах в вашем экземпляре Kaspersky SIEM Cloud. Вы можете отобразить или скрыть виджеты с помощью значка просмотра виджетов . Доступны следующие виджеты:

- **Статус пакетов** – количество пакетов со следующими статусами:
  - **Доступно** – пакет доступен для установки.
  - **Установлено** – пакет установлен целиком.
  - **Экстренно** – пакет содержит ресурсы с высоким приоритетом, которые необходимо установить как можно скорее.

- **Новое** – пакет добавлен в репозиторий менее трех месяцев назад и еще не был установлен или просмотрен.
- **Требуется обновление** – для пакета доступна более новая версия в репозитории.

  Для обновления пакета нужно повторно установить пакет. При повторной установке будет установлена доступная версия пакета.

- **Статус ресурсов** – количество ресурсов различных типов со следующими статусами:
  - **Доступно** – ресурс доступен для установки.
  - **Установлено** – ресурс установлен и не требует обновления.
  - **Требуется обновление** – для ресурса доступна более новая версия в репозитории.
- **Покрыто техниками MITRE, {{ filter }}** – информация о количестве или проценте техник MITRE ATT&CK, покрытых выбранными ресурсами.

Виджеты также являются фильтрами для таблиц на странице. При выборе значения в виджете таблица автоматически обновляется в соответствии с выбранным фильтром. Например, можно отобразить только ресурсы со статусом **Требуется обновление**.

При работе с таблицей доступны вкладки **Пакеты** и **Ресурсы.**

Описание вкладки Пакеты

На вкладке **Пакеты** отображается таблица со списком доступных пакетов, которая содержит следующие столбцы:

- **Название** – название пакета.
- **Версия** – версия пакета.
- **Дата выпуска** – дата выпуска пакета.
- **Типы ресурсов** – типы ресурсов, входящих в состав пакета:
  - Активный лист.
  - Контекстная таблица.
  - Нормализатор.
  - Правило агрегации событий.
  - Правило корреляции.
  - Правило обогащения.
  - Словарь.
  - Фильтр.
  - Шаблон уведомлений.

- **Количество ресурсов** – количество ресурсов в пакете.
- **Статус** – статус пакета:
  - **Доступно** – пакет доступен для установки.
  - **Установлено** – пакет установлен целиком.
  - **Экстренно** – пакет содержит ресурсы с высоким приоритетом, которые необходимо установить как можно скорее.
  - **Новое** – новый пакет, доступный для установки.
  - **Требуется обновление** – для пакета доступна более новая версия в репозитории.

    Для обновления пакета нужно повторно установить пакет. При повторной установке будет установлена доступная версия пакета.
- **Описание** — описание пакета.

Чтобы просмотреть информацию о пакете, нажмите на его название. Откроется окно с информацией о пакете, которое содержит вкладки **Общие** и **Журнал изменений**.

На вкладке **Общие** отображается следующая информация:

- название пакета;
- описание;
- дата выпуска;
- версия.

Также эта вкладка содержит блок **Импортируемые ресурсы**, в котором отображается список ресурсов, входящих в состав пакета. В блоке можно отфильтровать ресурсы и выбрать только необходимые для установки.

На вкладке **Журнал изменений** отображается информация об изменениях пакета, в том числе об изменениях всех ресурсов, входящих в пакет. Изменения сгруппированы по датам выпуска версий пакета.

Описание вкладки Ресурсы

На вкладке **Ресурсы** отображается таблица со списком доступных ресурсов, которая содержит следующие столбцы:

- **Название** – название ресурса.
- **Тип ресурса** – доступные типы ресурсов:
  - Активный лист.
  - Контекстная таблица.
  - Нормализатор.
  - Правило агрегации событий.

    - Правило корреляции.
    - Правило обогащения.
    - Словарь.
    - Фильтр.
    - Шаблон уведомлений.
- **Дата установки** – дата установки ресурса в Kaspersky SIEM Cloud.
- **Тенант** – тенант, в котором установлен ресурс.

  Если один и тот же ресурс установлен в нескольких тенантах, он отображается в таблице как группа. Чтобы просмотреть сведения об установленном ресурсе в каждом тенанте, нужно развернуть группу.
- **Версия** – версия ресурса.
- **Статус** – статус ресурса:
    - **Доступно** – ресурс доступен для установки.
    - **Установлено** – ресурс установлен.
    - **Требуется обновление** – для ресурса доступна новая версия.
- **Названия пакетов** – список пакетов, в которые входит ресурс.
- **Теги производителя** – теги, назначенные производителем ресурса.
- **Техники MITRE** – техники MITRE ATT&CK, связанные с ресурсом.

Чтобы просмотреть информацию о ресурсе, нажмите на его название. Откроется окно с информацией о ресурсе, которое содержит вкладки **Общая информация** и **Связанные ресурсы**.

На вкладке **Связанные ресурсы** вы можете просмотреть ресурсы, связанные с выбранным ресурсом. Вы также можете просмотреть зависимости на вкладке **Ресурсы** по кнопке **Показать зависимости**.

Для поиска пакетов или ресурсов используйте поле **Поиск**. Поиск выполняется только на открытой вкладке. При переключении между вкладками введенный поисковый запрос сохраняется и применяется к выбранной вкладке. В поле **Поиск** можно вводить название ресурса, источник событий, тип событий, название пакета или любую подстроку.

Для фильтрации содержимого вкладок **Пакеты** и **Ресурсы** нажмите значок фильтра .

Таблицы можно сортировать, нажав на заголовок столбца нужного параметра и выбрав **По возрастанию** или **По убыванию**. Также доступна фильтрация по столбцам **Тип ресурса** или **Статус**, нажав на заголовок необходимого столбца и выбрав значения, которые вы хотите отобразить.

Об импорте пакетов и ресурсов

Ресурсы импортируются в выбранный тенант. Связанные ресурсы, принадлежащие тенанту Shared, будут импортированы в тенант Shared. Права для учетной записи на тенант Shared не требуется. Нужны только права на импорт в выбранном тенанте.

Импортированные OOTB-ресурсы невозможно изменить или переместить. Если вы хотите изменить или переместить импортированный OOTB-ресурс, создайте его копию. При импорте следующих версий пакета копия не будет обновляться, поскольку представляет собой отдельный объект.

Импортированные ресурсы в папке `Integration` можно изменить. Подобные ресурсы отмечены **Этот ресурс входит в пакет**. К пакетному ресурсу в папке `Integration` допускается добавить словарь с типом `Таблица`. Добавить другие типы ресурсов невозможно. При импорте следующих версий пакета измененный ресурс не будет заменен на аналогичный ресурс из пакета, что позволит сохранить внесенные изменения.

Ресурсы из репозитория импортируются из репозитория на языке, указанном в параметре **Локализация ресурсов KUMA** в разделе параметров Ядра Kaspersky SIEM Cloud.

Установка пакетов

Пакет получает статус **Установлено** только в том случае, если установлены все ресурсы, входящие в его состав.

Чтобы установить пакет целиком:

1. Перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **База знаний** → **Пакеты**.
2. Выполните одно из следующих действий:
   - Установите флажок напротив нужного пакета и нажмите на кнопку **Установить**.
   - Нажмите на название пакета и в открывшемся окне нажмите на кнопку **Установить**.
3. Выберите тенант.
4. Нажмите на кнопку **Установить**.

Ресурсы будут импортированы в Kaspersky SIEM Cloud и доступны для дальнейшей настройки.

Установка отдельных ресурсов

Чтобы установить отдельные ресурсы из пакета:

1. Перейдите в раздел **Мониторинг → Ресурсы и сервисы → База знаний → Ресурсы**.
2. Выполните одно из следующих действий:
   - Установите флажок напротив нужных ресурсов и нажмите на кнопку **Установить**.
   - Нажмите на название ресурса и в открывшемся окне нажмите на кнопку **Установить**.
3. Выберите тенант.
4. Нажмите на кнопку **Установить**.

   Ресурс будет установлен.

Обновление ресурсов

Если для установленного ресурса доступна новая версия, ресурс получает статус **Требуется обновление**.

Чтобы обновить ресурс:

1. Перейдите в раздел **Мониторинг → Ресурсы и сервисы → База знаний → Ресурсы**.
2. Установите флажок напротив одного или нескольких ресурсов со статусом **Требуется обновление**.
3. Нажмите на кнопку **Обновить**.

Управление ресурсами и сервисами

Основными компонентами Kaspersky SIEM Cloud, с помощью которых решение осуществляет работу с событиями, являются *сервисы*. Сервисы позволяют получать события из источников, чтобы в дальнейшем привести их к общему формату, удобному для поиска корреляций, а также для хранения и ручного анализа. При создании каждому сервису присваивается идентификатор.

В Kaspersky SIEM Cloud доступны следующие типы сервисов:

- Хранилища – используются для хранения событий.
- Корреляторы – используются для анализа событий и поиска заданных закономерностей.
- Коллекторы – используются для получения события и конвертации их в формат Kaspersky SIEM Cloud.

- Агенты – используются для получения событий на удаленных устройствах и пересылки их в коллекторы.

- Маршрутизаторы событий – используются для приема потоков событий от коллекторов и корреляторов и дальнейшего распределения событий по указанным точкам назначения в соответствии с настроенными фильтрами.

Сервисы создаются на основе *ресурсов*. Ресурсы – это компоненты Kaspersky SIEM Cloud, которые содержат параметры для реализации различных функций, например, чтобы установить соединение с конкретным URL или преобразовать данные по определенным правилам. Ресурсы можно объединять в наборы ресурсов. При объединении ресурсов в набор они должны принадлежать к тому же тенанту, что и создаваемый набор ресурсов. Исключением является Общий тенант: принадлежащие ему ресурсы можно использовать в наборах ресурсов других тенантов.

Kaspersky SIEM Cloud поставляется с набором предустановленных ресурсов. Предустановленные ресурсы в названии содержат префикс **[OOTB]**. Такие ресурсы невозможно изменить. При этом вы можете создать копию предустановленного ресурса и внести изменения в копию.

Некоторые ресурсы связаны между собой. Например, в определенных типах коннекторов обязательно нужно указывать секрет коннектора. При импорте или экспорте таких коннекторов связанные секреты будут также импортированы или экспортированы.

В Kaspersky SIEM Cloud вы можете создавать следующие типы ресурсов:

- **Правила корреляции** – в ресурсах этого типа содержатся правила определения в событиях закономерностей, указывающих на угрозы. Если условия, заданные в этих ресурсах, выполняются, создается корреляционное событие.

- **Нормализаторы** – в ресурсах этого типа содержатся правила для приведения поступающих событий к формату, принятому в Kaspersky SIEM Cloud. После обработки в нормализаторе сырое событие становится нормализованным и может обрабатываться другими ресурсами и сервисами.

- **Коннекторы** – в ресурсах этого типа содержатся параметры для установления сетевых подключений.

- **Правила агрегации** – в ресурсах этого типа содержатся правила для объединения нескольких однотипных базовых событий в одно агрегационное событие.

- **Правила обогащения** – в ресурсах этого типа содержатся правила для дополнения событий информацией из сторонних источников.

- **Точки назначения** – в ресурсах этого типа содержатся параметры для пересылки событий в пункт дальнейшей обработки или хранения.

- **Фильтры** – в ресурсах этого типа содержатся условия для отбора отдельных событий из потока событий для дальнейшей их передачи в обработку.

- **Правила реагирования** – ресурсы этого типа используются в корреляторах для запуска, например, скриптов или задач Open Single Management Platform при выполнении определенных условий.

- **Правила сегментации** – ресурсы этого типа используются в корреляторах для разделения однотипных корреляционных событий по разным алертам.

- **Правила сбора и анализа данных** – в ресурсах этого типа содержатся правила, которые позволяют планировать выполнение SQL-запросов с агрегационными функциям в хранилище по заданному расписанию. Далее по данным, полученным от SQL-запросов, осуществляется корреляция.

- **Шаблоны уведомлений** – ресурсы этого типа используются при рассылке уведомлений о новых алертах.

- **Активные листы** – ресурсы этого типа используются коррелляторами для динамической работы с данными при анализе событий по правилам корреляции.
- **Словари** – ресурсы этого типа используются для хранения ключей и их значений, которые могут потребоваться другим ресурсам и сервисам Kaspersky SIEM Cloud.
- **Прокси-серверы** – в ресурсах этого типа содержатся параметры использования прокси-серверов.
- **Секреты** – ресурсы этого типа используются для безопасного хранения конфиденциальной информации (например, учетных данных), которые должны использоваться Kaspersky SIEM Cloud для взаимодействия с внешними службами.
- **Контекстные таблицы** – ресурсы этого типа используются коррелляторами Kaspersky SIEM Cloud для анализа событий в соответствии с правилами корреляции.
- **Панели мониторинга** – используются для контроля состояния безопасности сети организации. Панель мониторинга представляет собой набор виджетов, которые отображают аналитику данных безопасности.
- **Шаблоны отчетов** – используются для настройки регулярного формирования отчетов о состоянии процессов и объектов в сети организации. В шаблоне указываются запрос, параметры отображения данных и расписание формирования отчетов.

Ресурсы и сервисы располагаются в папках, которые можно добавлять, переименовывать, перемещать и удалять.

Общие инструкции по работе с ресурсами

В этом разделе описаны общие инструкции, как работать с ресурсами.

Чтобы просмотреть таблицу ресурса,

в главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → <тип ресурса>**.

Откроется таблица выбранного ресурса.

Ресурсы можно искать по названию с помощью поля **Поиск**. При поиске ресурсов используются регулярные выражения.

Таблицу можно сортировать по названию, дате и времени последнего обновления и тегам, нажав на значок сортировки ⌄ в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

Таблица содержит следующие столбцы:

- **Название** – название ресурса.
- **Последнее обновление** – дата и время последнего обновления ресурса.
- **Создал** – имя пользователя, создавшего ресурс.
- **Описание** – описание ресурса.
- **Тип** – тип ресурса. Отображается для всех типов ресурсов, кроме типов **Правила агрегации**, **Правила обогащения**, **Правила сбора и анализа данных**, **Фильтры**, **Активные листы**, **Прокси-серверы**.

- **Путь до ресурса** – папка в дереве ресурсов.
- **Теги** – теги, которыми отмечен ресурс. Ресурс может иметь больше одного тега. Теги являются частью ресурса и импортируются в случае импорта ресурса.
- **Название пакета** – имя пакета, из которого ресурс был импортирован из репозитория.
- **Коррелятор** – список корреляторов, к которым привязано правило корреляции. Отображается только для ресурсов типа **Правила корреляции**.

  Если правило не привязано ни к одному коррелятору, в столбце отображается пустое значение. Если в списке есть несколько значений, то эти значения отсортированы в алфавитном порядке. Вы можете фильтровать значения в столбце **Коррелятор**, нажав на заголовок столбца и выбрав, какие правила корреляции вы хотите просматривать в таблице: **Без коррелятора** или **С коррелятором**.

  Для правил тенанта Shared отображаются корреляторы тенантов, к которым у вас есть доступ и которые вы выбирали в списке тенантов.

  Значения в столбце **Коррелятор** доступны только для просмотра. Если вы хотите выполнить действия над корреляторами, вам нужно нажать на правило в таблице и в открывшихся свойствах этого правила перейти на вкладку **Корреляторы**.
- **Техники MITRE** – техники матрицы MITRE, которые покрывает это правило корреляции. Отображается только для ресурсов типа **Правила корреляции**. При наведении курсора мыши на значение отображается название правила.

При необходимости вы можете настроить отображение столбцов в таблице, нажав на значок шестеренки на значок шестеренки .

Максимальный размер таблицы не ограничен. Если вы хотите выбрать все ресурсы, прокрутите таблицу до конца и установите флажок **Выбрать все**, таким образом все доступные в таблице ресурсы будут выбраны.

В таблице ресурсов в нижней части отображается количество ресурсов из доступных вам тенантов в таблице:

- **Всего** – общее количество или с учетом примененного фильтра или поиска.
- **Выбрано** – количество выбранных ресурсов.

При применении фильтров выбранные ресурсы и значение **Выбрано** сбрасываются. Если количество ресурсов изменится из-за действий другого пользователя (например, удаление), отображаемое количество ресурсов изменится после того, как вы обновите страницу, выполните действие с ресурсом или примените фильтр.

Создание, дублирование, перемещение, редактирование и удаление ресурсов

В этой статье описано, как изменить, копировать и удалить ресурс.

Изменение ресурса

Чтобы изменить ресурс:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **<тип ресурса>**.
2. Нажмите на ресурс, который вы хотите изменить.

   Справа откроется панель с параметрами выбранного ресурса. Параметры зависят от типа ресурса.

3. Внесите необходимые изменения.

4. Сохраните изменения:

   - Нажмите **Сохранить**, чтобы сохранить изменения.

   - Нажмите **Сохранить с комментарием** и в открывшемся окне укажите комментарий к внесенным изменениям. Комментарий будет добавлен к созданной версии ресурса.

   Ресурс будет изменен, и для него будет создана новая версия. Если этот ресурс используется в сервисе, перезапустите сервис, чтобы он использовал новую версию ресурса.

   Если текущий ресурс недоступен для изменения (например, невозможно изменять корреляционные правила), можно перейти в карточку другого ресурса, нажав на кнопку **Посмотреть**. Эта кнопка становится доступной в пакетных ресурсах при нажатии на другой ресурс, связанный с текущим ресурсом.

Если при сохранении ресурса обнаруживается, что текущая версия ресурса была изменена другим пользователем, вам будут предложены следующие варианты:

- Сохранить ваши изменения как новую версию ресурса поверх изменений другого пользователя.

- Сохранить ваши изменения как новый ресурс.

  В этом случае будет создан дубликат изначального ресурса с измененными параметрами. В название нового ресурса будет добавлено `- копия`, и в комментарии к версии будут указаны название и версия ресурса, с которого был создан дубликат.

- Отменить ваши изменения.

  Отмененные изменения невозможно восстановить.

Создание ресурса на основе существующего

Чтобы создать копию ресурса:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **<тип ресурса>**.

2. Установите флажок рядом с ресурсом, который вы хотите копировать.

   Вы можете скопировать только один ресурс за раз.

3. В панели инструментов или в меню ⋮ нажмите **Дублировать**.

   Откроется панель с параметрами выбранного ресурса. Доступные параметры зависят от типа ресурса.

4. При необходимости в поле **Название** измените название ресурса.

   По умолчанию в поле отображается `<название выбранного ресурса> - копия`.

5. Измените нужные параметры.

6. Нажмите **Создать**.

   Ресурс будет создан на основе существующего.

Удаление ресурса

Чтобы удалить ресурс:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **<тип ресурса>**.

2. Установите флажки рядом с одним или несколькими ресурсами, которые вы хотите удалить.

   Чтобы выбрать несколько ресурсов одновременно, нужно установить флажок в заголовке первого столбца таблицы и выбрать один из вариантов:

   - **Выбрать все** – будут выбраны все ресурсы на всех страницах таблицы. Если ресурсы отфильтрованы с помощью поиска, будут выбраны все ресурсы, соответствующие условию поиска.

   - **Выбрать все на странице** – будут выбраны все ресурсы, отображаемые на открытой странице. Если ресурсы отфильтрованы с помощью поиска, будут выбраны все ресурсы на открытой странице, соответствующие условию поиска.

   В нижней части таблицы отобразится количество выбранных ресурсов.

3. В панели инструментов или в меню ⋮ нажмите **Удалить**.

   Откроется окно с информацией, можно ли удалить ресурсы, в зависимости от наличия связей выбранных для удаления ресурсов с другими ресурсами.

   Для всех ресурсов, которые невозможно удалить, существующие связи отобразятся в виде таблицы.

4. Подтвердите удаление ресурсов.

Ресурсы без связей и все сохраненные версии этих ресурсов будут удалены.

Привязка ресурсов к сервисам

Вы можете привязать правила корреляции, правила обогащения, правила реагирования, правила агрегирования и точки назначения к таким сервисам, как коллекторы, коррелляторы и маршрутизаторы событий. Доступные сервисы зависят от типа выбранного ресурса.

Чтобы привязать ресурс к сервису:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **<тип ресурса>**.

2. Установите флажки рядом ресурсами, которые вы хотите привязать.

3. В панели инструментов или в меню ⋮ нажмите **Привязать к сервису** → **Привязать к <название сервиса>**.

   Вы также можете привязать ресурс к сервису при изменении параметров ресурса. Для этого нажмите на название ресурса, перейдите на вкладку **Сервисы** и нажмите **Привязать к сервису** → **Привязать к <название сервиса>**.

> При изменении параметров правила корреляции доступна вкладка **Коррелляторы**, на которой вы можете привязать правило к коррелляторам.

Ресурс также можно привязать при создании или изменении параметров сервиса. Для этого в окне с параметрами сервиса перейдите в раздел, соответствующий типу ресурса, и добавьте нужный ресурс. Например, если вы хотите привязать к коллектору правило обогащения, перейдите в раздел **Обогащение событий** и добавьте правило по кнопке **Добавить обогащение**.

4. В открывшемся окне **<название сервиса>** установите флажки рядом с нужными сервисами и нажмите **OK**.

Ресурс будет привязан к сервису.

Чтобы отвязать ресурс от сервиса:

1. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → <тип ресурса>**.
2. Нажмите на ресурс и перейдите на вкладку **Сервисы**.

> Для правил корреляции отображается вкладка **Корреляторы**.

Ресурс также можно отвязать при изменении параметров сервиса. Для этого в окне с параметрами сервиса перейдите в раздел, в котором добавлен ресурс, и удалите его.

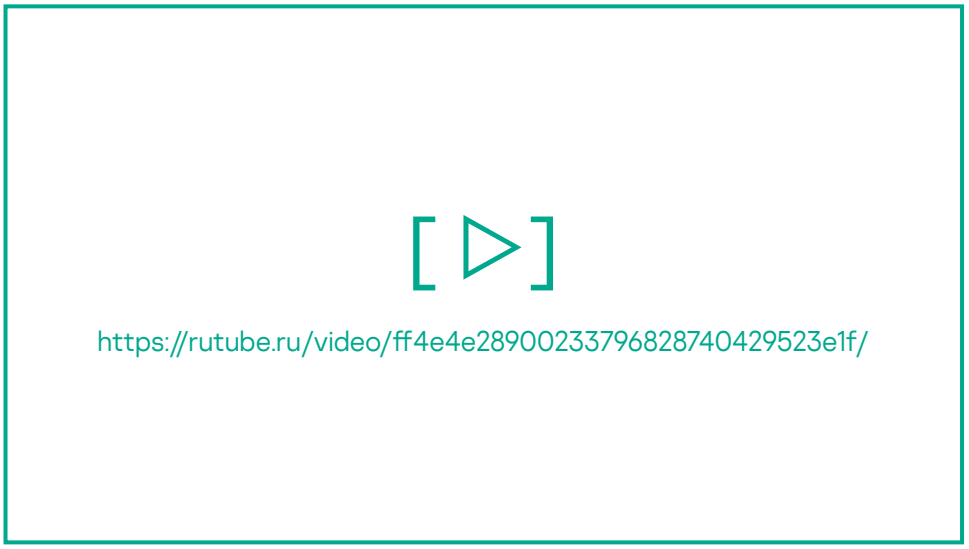
3. Установите флажки рядом с сервисами, от которых вы хотите отвязать ресурс.
4. Нажмите **Удалить** и подтвердите удаление привязки к сервису.

Ресурс будет отвязан от сервиса.

Обновление предустановленных ресурсов

Kaspersky SIEM Cloud поставляется с предустановленным набором ресурсов, таких как нормализаторы, правила корреляции и коннекторы. Специалисты "Лаборатории Касперского" регулярно обновляют эти ресурсы, например добавляют новые правила корреляции. Чтобы использовать актуальные версии ресурсов, вам нужно настроить их обновление.

В списке ресурсов предустановленные ресурсы маркируются с помощью префикса **[OOTB]**. Для наглядного ознакомления с процедурой обновления OOTB-ресурсов вы можете просмотреть видео ниже, а затем воспользоваться пошаговым сценарием.



https://rutube.ru/video/ff4e4e2890023379682874042952 3e1f/

Подсистема обновлений Kaspersky SIEM Cloud предоставляет механизмы для получения, хранения и использования ресурсов, необходимых для обработки событий и обнаружения угроз. Подсистема включает в себя два независимых механизма обновления:

- **Обновление хранилища** – механизм загрузки пакетов ресурсов с возможностью их просмотра, анализа и импорта в тенант.
- **Обновление OSMP** – автоматический механизм получения и использования ресурсов без участия пользователя и импорта вручную.

Оба механизма могут использовать следующие источники обновлений:

- Серверы обновлений "Лаборатории Касперского".
- Пользовательский источник (хранилище или зеркало обновлений).

Подсистема обновлений расширяет возможности Kaspersky SIEM Cloud для реагирования на изменения в картине угроз и инфраструктуре. Возможность использовать систему без прямого доступа в интернет помогает обеспечить конфиденциальность данных, обрабатываемых системой.

Обновление предустановленных ресурсов из репозитория состоит из следующих этапов:

1. Обновление репозитория

"Лаборатория Касперского" регулярно выпускает пакеты с ресурсами, доступные для импорта из репозитория. Вы можете указать адрес электронной почты в параметрах задачи **Обновление хранилища**. После первого выполнения задачи Kaspersky SIEM Cloud начинает рассылку уведомлений о доступных для обновления пакетах на указанный адрес.

Механизм обновления репозитория позволяет извлекать пакеты, просматривать их содержимое и принимать решение о развертывании их в операционной инфраструктуре. Обновление репозитория может производиться в автоматически или вручную.

При использовании в инфраструктуре других приложений "Лаборатории Касперского", можно подключить Kaspersky SIEM Cloud к уже существующем зеркалам обновления.

Чтобы настроить автоматическое обновление:

1. В главном окне приложения перейдите в раздел **Параметры → KUMA → Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Другое** нажмите **Параметры обновления**.

3. В блоке **Обновление репозитория** настройте **Период обновления данных в часах**. Значение по умолчанию – 24 часа.

4. Укажите **Источник обновления**. Доступны следующие параметры:

   - **Серверы обновлений "Лаборатории Касперского"**.

     Серверы расположены в разных странах по всему миру, что обеспечивает высокую надежность обновления. Если обновление невозможно выполнить с одного сервера, Kaspersky SIEM Cloud переключается на другой сервер.

     Вы можете посмотреть список серверов в Базе знаний.

- Пользовательский источник:
  - URL к папке общего доступа на HTTP-сервере.
  - Полный путь к локальной папке на устройстве с установленным ядром KUMA.

    В случае использования локальной папки у системного пользователя kuma должен быть доступ для чтения к этой папке и ее содержимому.

5. Укажите **Адреса электронной почты для рассылки уведомлений** для рассылки уведомлений, нажав на кнопку **Добавить**. На указанные адреса электронной почты будет поступать рассылка уведомлений о том, что в репозитории появились новые пакеты или новая версия тех пакетов, которые вы когда-либо импортировали в тенант.

   Если вы указываете электронную почту пользователя KUMA, в профиле пользователя должен быть установлен флажок **Получать уведомления по почте**. Для почты, которая не принадлежит ни одному пользователю KUMA, письмо будет приходит без дополнительных настроек. Параметры подключения к SMTP-серверу должны быть указаны во всех случаях.

6. Нажмите на кнопку **Сохранить**. Вскоре запустится задача обновления. Затем задача запускается по расписанию.

Чтобы запустить обновление репозитория вручную:

1. Если вы хотите выключить автоматическое обновление, в разделе **Параметры → KUMA → Открыть параметры KUMA → Параметры обновления → Обновление репозитория** включите переключатель **Отключить автоматическое обновление**. По умолчанию этот переключатель выключен. Также вы можете запустить обновление репозитория вручную, не отключая автоматическое обновление. Запуск обновления вручную не влияет на график выполнения автоматического обновления.

2. Укажите **Источник обновления**. Доступны следующие параметры:

   - **Серверы обновлений "Лаборатории Касперского"**.

     Серверы расположены в разных странах по всему миру, что обеспечивает высокую надежность обновления. Если обновление невозможно выполнить с одного сервера, Kaspersky SIEM Cloud переключается на другой сервер.

   - Пользовательский источник:
     - URL к папке общего доступа на HTTP-сервере.
     - Полный путь к локальной папке на устройстве с установленным ядром KUMA.

       В случае использования локальной папки у пользователя kuma должен быть доступ к этой папке и ее содержимому.

3. Укажите **Адреса электронной почты для рассылки уведомлений** для рассылки уведомлений, нажав на кнопку **Добавить**. На указанные адреса электронной почты будет поступать рассылка уведомлений о том, что в репозитории появились новые пакеты или новая версия тех пакетов, которые вы когда-либо импортировали в тенант.

   Если вы указываете электронную почту пользователя KUMA, в профиле пользователя должен быть установлен флажок **Получать уведомления по почте**. Для почты, которая не принадлежит ни одному пользователю KUMA, письмо будет приходит без дополнительных настроек. Параметры подключения к SMTP-серверу должны быть указаны во всех случаях.

4. Нажмите **Запустить обновление**. Таким образом, вы одновременно сохраните настройки и вручную запустите выполнение задачи **Обновление репозитория**.

❷ Обновление OSMP

Если это поддерживается лицензией, механизм обновления OSMP автоматически получает и использует ресурсы. Обновление OSMP выполняется автоматически в фоновом режиме и не требует импорта, анализа или одобрения пакетов вручную.

После завершения обновления новые поля событий и правила корреляции становятся доступными для обработки без дополнительной настройки.

Чтобы настроить обновление OSMP:

1. В главном окне приложения перейдите в раздел **Параметры → KUMA → Открыть параметры KUMA → Параметры обновления**.

2. Укажите **Источник обновления**. Доступны следующие параметры:

   - **Серверы обновлений "Лаборатории Касперского"**.

     Серверы расположены в разных странах по всему миру, что обеспечивает высокую надежность обновления. Если обновление невозможно выполнить с одного сервера, Kaspersky SIEM Cloud переключается на другой сервер.

   - Пользовательский источник:

     - URL к папке общего доступа на HTTP-сервере.

     - Полный путь к локальной папке на устройстве с установленным ядром Kaspersky SIEM Cloud.

       В случае использования локальной папки у пользователя kuma должен быть доступ к этой папке и ее содержимому. Если используется пользовательский источник, при необходимости настройте параметры прокси-сервера.

3. В блоке **Обновление OSMP** в поле **Период обновления данных в минутах** укажите период автоматической проверки и загрузки обновлений в минутах. Значение по умолчанию – 30.

4. Нажмите на кнопку **Сохранить**.

По умолчанию переключатель **Отключить автоматическое обновление** выключен, и обновление OSMP запускается автоматически в соответствии с интервалом указанным в поле **Период обновления данных в минутах**.

Если вы хотите выключить автоматическое обновление OSMP, включите переключатель **Отключить автоматическое обновление** и нажмите **Сохранить**. В этом случае автоматическая проверка обновлений и загрузка не выполняются. Чтобы запустить обновление OSMP вручную, нажмите **Запустить обновление**.

❸ Импорт ресурсов в тенант

После обновления репозитория импортируйте пакеты с ресурсами в тенант.

❹ Привязка ресурсов к сервисам

Чтобы сервисы начали использовать обновленные ресурсы, убедитесь, что ресурсы привязаны. При необходимости привяжите ресурсы к коллекторам, корреляторам или агентам и обновите параметры соответствующего сервиса.

Экспорт ресурсов

Если для пользователя скрыты общие ресурсы, невозможно экспортировать ни общие ресурсы, ни ресурсы, в которых используются общие ресурсы.

Чтобы экспортировать ресурсы:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы**.
2. В разделе **Ресурсы** нажмите **Экспортировать ресурсы**.

   Откроется окно **Экспортировать ресурсы**.
3. В поле **Пароль** введите пароль, который нужно использовать для защиты экспортируемых данных.

   Требования к паролю:

   - Должен содержать не менее 16 символов.
   - Должен содержать буквы в верхнем и нижнем регистрах, цифры и специальные символы (например, @, #, $).
   - Не должен содержать три или более одинаковых символа подряд.
4. В раскрывающемся списке **Тенант** выберите тенант, ресурсы которого вы хотите экспортировать.
5. Установите флажки рядом с ресурсами для экспорта.

   Если выбранные ресурсы связаны с другими ресурсами, эти ресурсы также будут экспортированы.

   В нижней части таблицы отобразится количество выбранных ресурсов.
6. Нажмите на кнопку **Экспортировать**.

Текущие версии ресурсов в защищенном паролем файле сохранятся на вашем компьютере в зависимости от параметров вашего браузера. Предыдущие версии ресурсов не будут сохранены в файле. Ресурсы секретов экспортируются пустыми.

Чтобы экспортировать предыдущую версию ресурса:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **<тип ресурса>**.
2. Установите флажок напротив ресурса, версию которого вы хотите экспортировать.
3. В панели инструментов или в меню ⋮ нажмите на кнопку **Показать историю версий**.

   Откроется окно с историей версий ресурса.

4. Нажмите на строку версии ресурса, которую вы хотите экспортировать, и затем нажмите на кнопку **Экспорт** в нижней части окна.

   Вы можете экспортировать только предыдущую версию ресурса. Кнопка **Экспорт** не отображается при выборе текущей версии ресурса.

Версия ресурса сохранится в файле JSON на вашем компьютере в зависимости от параметров вашего браузера.

Импорт ресурсов

В этой статье описывается процесс импорта ресурсов из файла. Ресурсы из репозитория вы можете импортировать в разделе **База знаний**.

Kaspersky SIEM Cloud поддерживает импорт ресурсов из более ранней версии в более позднюю.

При импорте нормализаторов поля расширенной схемы событий, используемые в нормализаторах, автоматически создаются в Kaspersky SIEM Cloud. Если такое поле уже существует в решении, при импорте будет использовано существующее поле.

Поля расширенной схемы событий создаются автоматически только на основании нормализаторов. Например, при импорте коллектора, содержащего нормализаторы, автоматически создаются все поля расширенной схемы, используемые этими нормализаторами. Поля, которые используются только в обогащениях или правилах корреляции и не используются в нормализаторах, автоматически не создаются в Kaspersky SIEM Cloud.

Чтобы импортировать ресурсы из файла:

1. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы**.
2. В разделе **Ресурсы** нажмите **Импортировать ресурсы**.

   Откроется окно **Импортировать ресурсы**.
3. Выберите файл, из которого вы хотите импортировать ресурсы, а также укажите пароль к этому файлу.
4. Нажмите **Импортировать**.
5. Если возникли конфликты между импортированными из файла и существующими ресурсами откроется **Конфликты**. По умолчанию в столбце **Родительский объект** отображается самый верхний родительский ресурс из выбранных при импорте.

   Выполните следующие действия:

   a. Если имя, тип и идентификатор (GUID) импортированных ресурсов полностью совпадает с именем, типом и/или идентификатором существующего ресурса, откроется окно **Конфликты** с таблицей, в которой отображаются тип и имя конфликтующих ресурсов. Разрешите отображаемые конфликты:

   - Если вы хотите заменить существующий ресурс новым, нажмите **Заменить**.

     Нажмите **Заменить все**, чтобы заменить все конфликтующие ресурсы. При этом все связанные ресурсы также будут автоматически заменены импортированными ресурсами.

   - Если вы хотите оставить существующий ресурс, нажмите **Пропустить**.

Вариант **Пропустить** недоступен для ресурсов, привязанных к другим ресурсам. Для таких ресурсов вы можете выбрать только вариант **Заменить**.

Нажмите **Пропустить все**, чтобы сохранить все существующие ресурсы.

b. Нажмите на кнопку **Устранить**.

Ресурсы будут импортированы в Kaspersky SIEM Cloud. Ресурсы секретов импортируются пустыми. В случае конфликта импортируемые ресурсы будут добавлены в качестве новой версии существующего ресурса. К этой версии будет добавлен комментарий `ресурс импортирован`.

Поиск ресурсов

Вы можете искать ресурсы по названию или тегам. Также можно использовать полнотекстовый поиск для поиска ресурсов по всем их полям. Для типа ресурсов **Правила корреляции** доступен полнотекстовый поиск по корреляторам, в которых используются правила. При поиске по фильтру будут найдены все ресурсы, которые его используют.

Поиск осуществляется только по последней версии ресурсов.

Чтобы найти нужные ресурсы:

1. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → <тип ресурса>**.

   Откроется окно с таблицей доступных ресурсов этого типа.

   Если вы хотите просмотреть все ресурсы, в разделе **Ресурсы и сервисы** перейдите на вкладку **Список**.

2. При необходимости переключите режим поиска. Для этого нажмите на значок таблицы в верхней части таблицы ресурсов.

   Доступны поиск по названию, тегам и полнотекстовый поиск по всем полям ресурса. По умолчанию активен поиск по названию, тегам и корреляторам (только для правил корреляции).

   Вы можете определить, какой режим поиска активен, по тексту, который отображается в поле поиска по умолчанию.

3. В поле **Поиск** начните вводить текст поиска.

   Поиск инициируется во время ввода символов в поле и не чувствителен к регистру.

   В таблице отображаются только те ресурсы, которые удовлетворяют условиям поиска В нижней части таблицы отображается количество таких ресурсов.

   Для полнотекстового поиска результаты отсортированы по количеству слов в поисковой строке, найденных в полях ресурса, от большего к меньшему. Kaspersky SIEM Cloud выполняет поиск по JSON ресурса. Если в нем указан другой ресурс, выполняет поиск по указанному ресурсу тоже. Если ресурс ссылается на другие ресурсы, Kaspersky SIEM Cloud также переходит в эти ресурсы и ищет по их содержимому.

4. Если вы хотите сбросить результат поиска, очистите поле **Поиск** или нажмите на значок ×.

Просмотр сервисов Kaspersky SIEM

Чтобы просмотреть таблицу сервисов:

1. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.

2. Если вы хотите обновить таблицу, нажмите на кнопку **Обновить**.

Сервисы можно искать по названию с помощью поля **Поиск**. При поиске сервисов используются регулярные выражения.

Таблицу можно сортировать по статусу, типу, названию сервиса, версии, тенанту, полному доменному имени, IP-адресу и порту API, нажав на значок сортировки ⌄ в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

Таблица сервисов содержит следующие столбцы:

- **Статус** – статус сервиса:
  - Зеленый – сервис работает и доступен с сервера Ядра Kaspersky SIEM Cloud.
  - Красный – сервис не работает или не доступен с сервера Ядра Kaspersky SIEM Cloud.
  - Желтый – сервис работает, но в журнале сервиса есть ошибки или для сервиса есть алерты от Victoria Metrics. Сообщение об ошибке отображается, если навести курсор мыши на статус сервиса. Желтый статус применяется ко всем сервисам, кроме агента.
  - Фиолетовый – изменился конфигурационный файл сервиса, но другие ошибки отсутствуют. Если у сервиса некорректный конфигурационный файл и есть ошибки, например от Victoria Metrics, статус сервиса будет желтым.
  - Серый – в удаленном тенанте был работающий сервис, который продолжает работать. Сервисы в сером статусе остаются после удаления тенанта, чтобы вы могли скопировать идентификатор и удалить сервисы на серверах. Удалить сервисы с серым статусом может только Главный администратор. При удалении тенанта сервисы этого тенанта привязываются к тенанту Main.
- **Тип** – вид сервиса: **ядро, агент**, **коллектор**, **коррелятор**, **хранилище**, **маршрутизатор событий**.
- **Название** – название сервиса. При нажатии на название сервиса открываются его параметры.
- **Версия** – версия сервиса.
- **Тенант** – название тенанта, которому принадлежит сервис.
- **Полное доменное имя** – доменное имя сервера, на котором установлен сервис.
- **IP-адрес** – IP-адрес сервера, на котором установлен сервис.
- **Порт API** – номер порта для внутренних коммуникаций.
- **Время работы** – время работы сервиса.

- **Создан** – дата и время создания сервиса.
- **UUID** – уникальный идентификатор сервиса.

При необходимости вы можете настроить отображение столбцов в таблице, нажав на значок шестеренки на значок шестеренки .

Общие инструкции по работе с сервисами

В этом разделе приведены общие инструкции по работе с сервисами.

Изменение названия сервиса

При необходимости вы можете изменить имя и параметры созданных сервисов.

Чтобы изменить имя сервиса:

1. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
2. Нажмите на ссылку с названием сервиса в столбце **Сервис**.
3. В открывшемся окне укажите новое название сервиса и при необходимости измените параметры. Имя должно быть уникальным в рамках одного тенанта и содержать от 1 до 128 символов в кодировке Unicode.

   Для сервисов Ядро Kaspersky SIEM Cloud и сервиса Метрики доступно только изменение имени.
4. Нажмите на кнопку **Сохранить**.

Получение идентификатора сервиса

При создании каждому сервису присваивается идентификатор, который затем используется, например, при установке сервиса на сервере.

Чтобы получить идентификатор сервиса:

1. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
2. В контекстном меню сервиса, идентификатор которого вы хотите получить, выберите **Копировать идентификатор**.

Идентификатор сервиса будет скопирован в буфер.

Остановка, запуск, проверка статуса сервиса

Чтобы остановить, запустить или проверить статус Ядра Kaspersky SIEM Cloud:

1. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
2. В контекстном меню сервиса выберите **Копировать идентификатор**.

   Идентификатор будет скопирован в буфер обмена.
3. В командной строке выполните одну из следующих команд:

   Остановка сервиса

   ```
   sudo systemctl stop kuma-core/collector/correlator/storage/metrics-<service_ID>.service
   ```

   Запуск сервиса

   ```
   sudo systemctl start kuma-<collector/correlator/storage/eventRouter/metrics>-<service_ID>.service
   ```

   Проверка статуса сервиса

   ```
   sudo systemctl status kuma-<collector/correlator/storage/eventRouter/metrics>-<service_ID>.service
   ```

   Где:

   <service_ID> – идентификатор сервиса, скопированный в буфер обмена.

Остановка, запуск, проверка статусов агентов под управлением Windows

Чтобы остановить или запустить агент под управлением Windows:

1. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
2. В контекстном меню агента, идентификатор которого вы хотите получить, выберите **Копировать идентификатор**.

   Идентификатор будет скопирован в буфер обмена.
3. Подключитесь к хосту, на котором требуется запустить или остановить агент Kaspersky SIEM Cloud.
4. Запустите интерпретатор команд PowerShell от имени учетной записи с правами администратора.

5. В PowerShell выполните одну из следующих команд:

```
Остановка агента
```

```
Stop-Service -Name "WindowsAgent-<идентификатор агента>"
```

```
Запуск агента
```

```
Start-Service -Name "WindowsAgent-<идентификатор агента>"
```

Чтобы просмотреть статус агента:

1. В Windows откройте приложение **Службы** (**Services**).
2. В списке служб двойным щелчком мыши откройте агент Kaspersky SIEM Cloud, статус которого вы хотите просмотреть.
3. В открывшемся окне на вкладке **Общие** (**General**) просмотрите статус в поле **Состояние** (**Service status**).

Обновление и перезапуск сервиса

Чтобы обновить или перезапустить сервис:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**.
2. Установите флажок рядом с сервисом и выберите один из следующих вариантов:
   - Если нужно обновить параметры работающего сервиса без его остановки, например для изменения параметров сопоставления полей или параметров точки назначения, выберите **Обновить параметры**.
   - Если нужно остановить сервис и запустить заново, например для изменения порта или типа коннектора, выберите **Перезапустить**.

     Особенности перезапуска агентов Kaspersky SIEM Cloud:

     - Агент Kaspersky SIEM Cloud для Windows можно перезапустить, только если он запущен на удаленном компьютере. Если сервис на удаленном компьютере неактивен, при попытке перезагрузить его из Kaspersky SIEM Cloud отобразится сообщение об ошибке. В этом случае следует перезапустить сервис Агент Kaspersky SIEM Cloud для Windows на удаленном компьютере с Windows. Чтобы узнать, как перезапустить сервисы Windows, обратитесь к документации, относящейся к версии операционной системы вашего удаленного компьютера с Windows.
     - Агент Kaspersky SIEM Cloud для Linux при использовании этой опции останавливается. Для запуска агента необходимо выполнить команду, с помощью которой он был запущен.

Удаление сервиса

Чтобы удалить сервис:

1. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
2. Получите идентификатор удаляемого сервиса. Для этого контекстном меню сервиса нажмите **Копировать идентификатор**.
3. В контекстном меню сервиса нажмите **Удалить**.
4. Подтвердите удаление.
5. Удалить сервис на сервере, выполнив следующую команду:

   ```
   sudo /opt/kaspersky/kuma/kuma <collector/correlator/storage/eventRouter/metrics> --core https://<FQDN>:<port> --id <service_ID> --uninstall
   ```

   Где:

   - <FQDN> — полное доменное имя сервера Ядра Kaspersky SIEM Cloud.
   - <port> — порт, используемый ядром KUMA для внутренних коммуникаций (по умолчанию 7210).
   - <service_ID> — идентификатор сервиса, скопированный в веб-интерфейсе Kaspersky SIEM Cloud.

   Например:

   ```
   sudo /opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --id 29fd6760-a870-42d2-8ebe-eb911ac90305 --uninstall
   ```

Сервис будет удален.

Установка дополнительных ресурсов и сервисов

При выборе автоматического развертывания при активации решения Kaspersky SIEM Cloud развертывается в типовой конфигурации. При необходимости вы можете добавить в конфигурацию дополнительные ресурсы и сервисы.

Ресурсы вы можете добавлять бесплатно. Сервисы вы можете установить только при наличии у вас достаточного количества вычислительных единиц:

- Коллекторы.
- Коррелеторы.
- Хранилища.
- Маршрутизаторы событий.

О вычислительных единицах

Вычислительная единица – это унифицированная единица измерения вычислительных ресурсов, таких как мощность процессора, количество оперативной памяти или размер хранилища. При покупке лицензионного ключа вы получаете некоторое количество вычислительных единиц, соответствующее вашей лицензии. Эти вычислительные единицы вы можете использовать для расширения конфигурации Kaspersky SIEM Cloud, например для установки дополнительного коррелятора или хранилища.

При выборе и настройке сервиса Kaspersky SIEM Cloud отображает "стоимость" сервиса в вычислительных единицах. Для дальнейшего развертывания сервиса в облачной инфраструктуре у вас должно быть достаточное количество вычислительных единиц. При недостаточном количестве вычислительных единиц развертывание сервиса невозможно.

Ваш текущий баланс доступных и использованных вычислительных единиц отображается в разделе **Мониторинг → Ресурсы и сервисы → Активные сервисы** в правой части экрана. Вы можете купить дополнительные вычислительные единицы. Для этого вам нужно приобрести лицензию Kaspersky Cloud Compute Unit.

При добавлении сервиса вычислительные единицы резервируются. При удалении сервиса вычислительные единицы, зарезервированные для его развертывания, освобождаются и становятся доступными для использования.

Добавление сервисов с использованием вычислительных единиц

Чтобы добавить сервис с использованием вычислительных единиц:

1. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → <тип сервиса>**.
2. Создайте и настройте сервис: коллектор, коррелятор, хранилище или маршрутизатор событий.
3. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → Активные сервисы**.
4. Нажмите на кнопку **Добавить**, затем выберите **Добавить сервис**.

   Откроется окно **Выберите сервис**.
5. Установите флажок рядом с созданным сервисом, затем нажмите **Создать сервис**.

   Сервис добавляется в список активных сервисов.
6. Установите флажок рядом с созданным сервисом и нажмите на кнопку **Развернуть**.

   Откроется панель с параметрами выбранного сервиса. Доступные параметры зависят от типа сервиса.
7. Выберите шаблон сервиса и укажите другие параметры.

   Kaspersky SIEM Cloud отображает количество вычислительных единиц, необходимых для установки сервиса в выбранной конфигурации. Если вам не хватает доступных вычислительных единиц, либо измените параметры сервиса, либо приобретите дополнительные вычислительные единицы.
8. Нажмите **Развернуть**.

Сервис создан и установлен в облачной инфраструктуре.

Версионирование ресурсов и сервисов

Kaspersky SIEM хранит историю изменения ресурсов и сервисов в виде версий. Версия создается автоматически, когда вы создаете ресурс или сервис либо изменяете параметры существующего.

История изменений недоступна для словарей. Для хранения истории изменения словарей вы можете экспортировать данные.

Версии хранятся в течение срока, указанного в разделе **Параметры**. Когда срок хранения версии достигает указанного значения, версия удаляется автоматически.

Вы можете просматривать историю изменений ресурсов и сервисов, сравнивать версии, а также восстановить предыдущую версию, например, когда нужно восстановить работоспособность ресурса.

Просмотр версии

Чтобы просмотреть историю изменений ресурса или сервиса:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **<тип ресурса или сервиса>**.

   Если вы хотите просмотреть все ресурсы и сервисы, в разделе **Ресурсы и сервисы** откройте вкладку **Список**.

2. Установите флажок рядом с ресурсом или сервисом, историю изменений которого вы хотите просмотреть.

3. В панели инструментов или в меню ⋮ нажмите **Показать историю версий**.

   Откроется таблица версий.

Вы можете отсортировать таблицу версий по столбцам **Версия**, **Опубликовано** и **Автор**, нажав на заголовок и выбрав **По возрастанию** или **По убыванию**. Вы также можете отобразить в таблице изменения, сделанные только конкретными пользователями, нажав на заголовок столбца **Автор** и выбрав нужных пользователей.

Таблица содержит следующие столбцы:

- **Версия** – порядковый номер версии. При изменении ресурса или сервиса и создании новой версии порядковый номер увеличивается на 1.

  Версия с наибольшим номером и недавней датой публикации соответствует актуальному состоянию. Версия 1 отражает состояние ресурса или сервиса при его создании.

- **Опубликовано** – дата и время, когда версия была создана.

- **Автор** – имя пользователя, сохранившего изменения.

  Если изменения были сделаны Kaspersky SIEM или с помощью скрипта миграции, отображается **system**.

- **Комментарий** – текстовый комментарий, указанный при сохранении изменений, или системный комментарий, описывающий сделанные изменения.

- **Срок хранения** – количество дней и дата, после которых версия будет удалена.

  При необходимости вы можете настроить срок хранения версий.

- **Действия** – кнопка восстановления версии.

Если вы хотите просмотреть состояние ресурса или сервиса в конкретной версии, нажмите на эту версию в таблице. В открывшемся окне вы можете выполнять следующие действия:

- просмотреть параметры выбранной версии;
- восстановить версию, нажав на кнопку **Восстановить**;
- экспортировать версию в JSON-файл, нажав на кнопку **Экспорт**.

Сравнение версий ресурса

Вы можете сравнивать любые две версии, например, если вам нужно отслеживать внесенные изменения.

Чтобы сравнить версии:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **<тип ресурса или сервиса>**.

   Если вы хотите просмотреть все ресурсы и сервисы, в разделе **Ресурсы и сервисы** откройте вкладку **Список**.

2. Установите флажок рядом с ресурсом или сервисом, версии которого вы хотите сравнить
3. В панели инструментов или в меню ⋮ нажмите **Показать историю версий**.

   Откроется таблица версий.

4. Установите флажки рядом с версиями, которые вы хотите сравнить, и нажмите на кнопку **Сравнить**.

Отобразится сравнение версий. Поля ресурсов или сервисов отобразятся в виде списка или в формате JSON. Различия между двумя версиями будут выделены цветом. Вы можете выбрать другие версии для сравнения с помощью раскрывающихся списков.

Восстановление версии ресурса

Вы можете восстановить предыдущую версию ресурса или сервиса, например, когда вам нужно восстановить работоспособность ресурса в случае ошибок при внесении изменений.

> Версии автоматически созданных агентов невозможно восстановить отдельно, так как они создаются при изменении родительского коллектора. Если вы хотите восстановить версию автоматически созданного агента, вам нужно восстановить соответствующую версию родительского коллектора.

Чтобы восстановить предыдущую версию:

1. В главном окне приложения перейдите в раздел **Мониторинг → Ресурсы и сервисы → <тип ресурса или сервиса>**.

   Если вы хотите просмотреть все ресурсы и сервисы, в разделе **Ресурсы и сервисы** откройте вкладку **Список**.

2. Установите флажок рядом с ресурсом или сервисом, версию которого вы хотите восстановить.

3. В панели инструментов или в меню ⋮ нажмите **Показать историю версий**.

   Откроется таблица версий.

4. В строке нужной версии в столбце **Действие** нажмите **Восстановить**.

   Вы можете восстановить версию, нажав на строку этой версии и затем нажав на кнопку **Восстановить** в нижней части окна.

   > Вы можете восстановить только предыдущие версии. Для текущей версии кнопка **Восстановить** недоступна.

   > Если после обновления Kaspersky SIEM изменилась структура ресурса или сервиса, восстановление сохраненных версий может быть недоступно.

5. Подтвердите действие и при необходимости укажите комментарий. Если вы не укажете комментарий, к версии автоматически будет добавлен комментарий `Восстановлена из версии v.<номер восстанавливаемой версии>`.

Версия будет восстановлена как новая версия и станет текущей. Если ресурс, версию которого вы восстановили, добавлен в активный сервис, состояние сервиса также изменится. Необходимо перезагрузить сервис, чтобы применить изменение ресурса.

Настройка срока хранения версий

> Только пользователь с ролью Главный администратор может просматривать и изменять срок хранения версий.

Чтобы изменить срок хранения версий:

1. В главном окне приложения перейдите в раздел **Параметры → KUMA → Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Другое → Общее** измените значение параметра **Срок хранения истории ресурсов, дни**.

По умолчанию установлено значение 30 дней. Если вы хотите хранить все версии без ограничений по сроку, вы укажите `0` (бессрочное хранение).

Срок хранения версий проверяется ежедневно, и версии, которые хранятся в Kaspersky SIEM дольше указанного срока, удаляются автоматически. В разделе **Диспетчер задач** создается задача *Очистка истории изменений ресурсов* для проверки срока хранения версий и удаления старых версий. Эта задача также запускается после перезапуска Ядра Kaspersky SIEM Cloud.

Вы можете проверить время, оставшееся до удаления версии, в таблице версий в столбце **Срок хранения**.

Просмотр графа зависимостей

Для устойчивой работы решения важно понимать, как одни ресурсы и сервисы влияют на работоспособность других, какие связи есть между ресурсами и другими объектами Kaspersky SIEM Cloud. Эти взаимозависимости вы можете просмотреть на интерактивном графе в веб-интерфейсе решения.

Отображение зависимостей на графе

Чтобы просмотреть граф зависимостей:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **<тип ресурса или сервиса>**.

   Если вы хотите просмотреть все ресурсы и сервисы, в разделе **Ресурсы и сервисы** откройте вкладку **Список**.

2. Установите флажок рядом с ресурсом или сервисом, связи которого вы хотите просмотреть.

3. В панели инструментов или в меню ⋮ нажмите на кнопку **Показать зависимости**.

   Откроется граф зависимостей. Для просмотра нужной части графа, используйте карту графа в правом нижнем углу.

   С помощью поля **Поиск** вы можете найти нужный узел по имени, тегу, пути или пакету.

4. Если вы хотите скачать данные о зависимостях, нажмите на кнопку **Скачать в формате SVG**.

5. При необходимости настройте фильтры для отображения зависимостей на графе с помощью раскрывающегося списка **Показывать на графе**.

Типы связей на графе

На графе отображаются все связи, которые формируются на основе универсального уникального идентификатора (UUID) ресурсов, используемых в конфигурации выбранного ресурса или сервиса, а также связи ресурсов, которые имеют UUID выбранного ресурса в своей конфигурации. Связи, на которые ссылается (использует) выбранный ресурс или сервис, показываются до последнего уровня. Связи, которые ссылаются на выбранный ресурс или сервис, отображаются только на один уровень.

Типы связей:

- Сплошная линия без надписи.

  Показывает прямую связь по UUID, в том числе использование секретов и прокси-серверов в интеграциях.

- Линия с надписью **<имя_функции>**.

  Показывает использование активного листа в правиле корреляции.

- Пунктирная линия с надписью **linked**.

  Показывает связь по URL, например точки назначения с коллектором или точки назначения с хранилищем.

Ресурсы, отображаемые на графе

На графе вы можете посмотреть связи следующих ресурсов:

правила корреляции;

правила агрегации;

правила обогащения;

правила реагирования;

правила сбора и анализа данных;

нормализаторы;

коннекторы;

точки назначения;

фильтры;

панели мониторинга;

Панели мониторинга не входят в состав других ресурсов, поэтому отсутствуют связи с ресурсами, которые ссылаются на панели мониторинга.

шаблоны отчетов;

Шаблоны отчетов не входят в состав других ресурсов, поэтому отсутствуют связи с ресурсами, которые ссылаются на шаблоны отчетов.

шаблоны уведомлений;

активные листы;

словари;

прокси-серверы;

секреты;

контекстные таблицы;

коллекторы;

Если для отображения связей изначально был выбран коллектор, то не отображаются связи с ресурсами, которые ссылаются на этот коллектор.

коррелляторы;

хранилища;

агенты (автоагенты);

Если для отображения связей выбран агент, то коллектор отображается с типом связи **linked**, только если коллектор запущен как сервис и в агенте коллектор корректно (FQDN и порт) указан в точке назначения.

маршрутизаторы событий;

Если для отображения связей изначально был выбран маршрутизатор событий, то не отображаются связи с ресурсами, которые ссылаются на этот маршрутизатор событий.

интеграции;

Название интеграции соответствует названию вкладки в разделе **Интеграции**.

недоступный ресурс (при отсутствии прав на просмотр).

При нажатии на узел ресурса отображаются следующие данные о ресурсе: **Имя**, **Тип**, **Путь**, **Теги**, **Тенант**, **Название пакета**. При нажатии на имя откроется информация о ресурсе или сервисе в отдельной вкладке.

Настройка отображения узлов и связей на графе

Отображение узлов и связей на графе выполняется в контекстом меню узла, в котором доступны следующие действия:

- **Показать зависимости ресурса**.

  Отобразятся зависимости ресурса и/или сервиса.

- **Скрыть ресурс**.

  Ресурс будет скрыт. Связанные ресурсы или сервисы будут отмечены значком ссылки ( ). Связи на графе будут разорваны.

- **Скрыть ресурсы этого типа**.

  Все ресурсы выбранного типа будут скрыты.

- **Скрыть связи ресурса**.

  Ресурс или сервис будет отмечен значком ссылки () как имеющий скрытые связи.

- **Обновить связи ресурса**.

  Будут обновлены видимые связи, которые изменились во время работы с графом.

- **Сгруппировать**.

  Действие доступно при наличии более десяти однотипных ссылок на ресурс.

Управление тегами

Для работы с ресурсами в веб-интерфейсе Kaspersky SIEM Cloud предусмотрена возможность добавлять теги для ресурсов. Вы можете выполнять поиск нужного компонента, а также управлять тегами, назначать теги или отменять назначение тегов.

Невозможно добавлять теги в ресурсы, которые создаются из интерфейса других ресурсов. Теги можно добавлять только из карточки самого ресурса. Также невозможно добавлять теги к ресурсу, недоступному для редактирования.

Управление тегами

Список тегов отображается в разделе **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Теги** и представлен в виде таблицы со столбцами **Название**, **Тенант**, **Использовано в ресурсах**.

В таблице **Теги** вы можете выполнять следующие действия:

- Сортировать теги по полям **Название**, **Использовано в ресурсах**.
- Фильтровать значения поля **Тенант**.
- Осуществлять поиск тега по полю **Название**.
- Переходить к списку ресурсов по выбранному тегу.

Добавление тега

Чтобы добавить тег:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** и выберите ресурс.
2. В панели над таблицей нажмите **Добавить**.
3. В поле **Теги** выбранного ресурса добавьте новый тег или выберите тег из списка.
4. Нажмите на кнопку **Создать**.

Новый тег будет добавлен.

Вы также можете добавлять теги из уже существующих.

При добавлении тега следует учитывать следующие особенности:

- Вы можете добавить несколько тегов.
- Тег может содержать буквы различных алфавитов (например, символы кириллицы, латиницы или греческого алфавита), цифры, знак нижнего подчеркивания и пробел.
- Тег не может содержать другие специальные символы, кроме нижнего подчеркивания и пробела.
- Вы можете вводить тег в любом регистре, но после сохранения тег будет всегда отображаться в нижнем регистре.
- Тег наследует тенант ресурса, в котором используется.
- Тег является частью ресурса и существует, пока существует ресурс, в котором тег был создан или используется.
- Теги уникальны в рамках тенанта.
- Теги импортируются или экспортируются вместе с ресурсом как часть ресурса.

Поиск по тегам

В разделе **Ресурсы** вы можете осуществить поиск ресурсов:

- По тегам.
- По наименованию ресурсов.

Поиск осуществляется по всем типам ресурсов и служб.

В результате поиска отображается список ресурсов и служб.

Чтобы найти нужные ресурсы по тегам:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** и выберите ресурс.
2. В таблице ресурса выберите столбец **Теги**.
3. В появившемся поле **Поиск** введите или выберите название тега.

   Поиск по тегу в самом ресурсе и в списке ресурсов осуществляется как при полном, так и частичном совпадении введенного текста с названием тега.

Отображается список ресурсов, если в этих ресурсах используется указанный тег.

В списке ресурсов вы можете выполнять следующие действия:

- Сортировать список по наименованию, типу ресурса или службы.
- Фильтровать ресурсы или службы по типу ресурса или службы, тегу.
- Назначать теги или отменять назначение тегов.

Отображение тегов при добавлении зависимых ресурсов

При добавлении зависимого ресурса в раскрывающемся списке отображаются теги этого ресурса в разделе **Параметры фильтра**.

Теги ресурса, которые не помещаются в одну строку, скрываются. На наличие скрытых тегов указывает специальный признак.

Раскрывающийся список можно фильтровать по названию ресурса и по тегам ресурса.

Назначение тегов или отмена назначения тегов

Чтобы назначить теги ресурсу или отменить назначение тегов ресурсу:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы**.
2. Выберите вкладку **Список**.
3. В столбце **Название** установите флажки рядом с нужными ресурсами.
4. В панели над списком выберите вкладку **Теги**.
5. Нажмите на кнопку **Привязать** или **Отвязать**, выберите нужные теги или создайте тег.

   Выбранные теги будут назначены ресурсам или назначение тегов ресурсам будет удалено.

   Вы также можете привязать или отвязать теги в карточке ресурса.

Управление папками

Ресурсы можно расположить по папкам. В левой части окна отображается структура папок, где корневые папки соответствуют тенантам и содержат перечень всех ресурсов тенанта. Во вложенных папках отображаются ресурсы этой папки. Когда папка выбрана, содержащиеся в ней ресурсы отображаются в таблице в правой части окна.

Папки можно создавать, переименовывать, добавлять в избранное, перемещать и удалять. Также вы можете перемещать ресурсы между папками.

Создание папки

Чтобы создать папку:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **<тип ресурса или сервиса>**.
2. В дереве выберите папку тенанта, в которой требуется создать вложенную папку.

3. Нажмите на значок плюса ＋.
4. В открывшемся окне укажите название папки и нажмите **Добавить**.

Папка будет создана.

Изменение папки

Чтобы переименовать папку:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы**.
2. Выберите ресурс или сервис, папку которого вы хотите переименовать.
3. В дереве наведите курсор на название папки.
4. В меню ⋮ справа выберите **Переименовать**.
5. Введите новое название папки и сохраните изменения.

Папка будет переименована.

Добавление папки в избранное

Чтобы добавить папку в избранное:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **<тип ресурса или сервиса>**.
2. В дереве наведите курсор на название папки, которую вы хотите добавить в избранное.
3. В меню ⋮ справа выберите **В избранное**.

   Папка будет добавлена в избранное.
4. Если вы хотите убрать папку из избранного, в меню ⋮ справа выберите **Убрать из избранного**.

Папка будет добавлена в избранное

Перемещение папки

> Папки невозможно переместить из одного тенанта в другой.

Чтобы переместить папку:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **<тип ресурса или сервиса>**.
2. В дереве нажмите название папки и перетащите ее в нужное место в структуре папок.

Папка будет перенесена.

Перемещение ресурсов или сервисов

Вы можете перемещать ресурсы только в папки того тенанта, для которого были созданы ресурсы. Перемещать ресурсы в папки другого тенанта невозможно.

Чтобы переместить ресурс или сервис в другую папку:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **<тип ресурса или сервиса>**.
2. Установите флажки рядом с ресурсами или сервисами, которые вы хотите переместить.

   В нижней части таблицы отобразится количество выбранных ресурсов.
3. Перетащите ресурсы в нужную папку с ⣿.

Ресурсы или сервисы будут перемещены.

Удаление папки

Папку можно удалить, даже если она содержит вложенные папки, ресурсы или сервисы. Перед удалением необходимо подтвердить действие, введя сгенерированное значение. При наличии зависимых ресурсов в папке в окне подтверждения отображается список зависимостей.

Чтобы удалить папку:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **<тип ресурса или сервиса>**.
2. В дереве наведите курсор на название папки, которую вы хотите удалить.
3. В меню ⋮ справа выберите **Удалить**.
4. Введите сгенерированное значение.
5. Подтвердите удаление.

Папка будет удалена.

Уведомления Kaspersky SIEM Cloud

В Kaspersky SIEM Cloud можно настроить отправку уведомлений по электронной почте с помощью SMTP-сервера. Для этого необходимо настроить подключение к SMTP-серверу, а также установить флажок **Получать уведомления по почте** для пользователей, которым должны приходить уведомления.

Kaspersky SIEM Cloud автоматически уведомляет пользователей о следующих событиях:

- Создан отчет (уведомление получают пользователи, перечисленные в параметрах расписания шаблона отчета).
- Выполнена задача (уведомление получают пользователи, создавшие задачу).
- Доступны новые пакеты с ресурсами. Их можно получить путем обновления хранилища Kaspersky SIEM Cloud (уведомление получают пользователи, чей адрес электронной почты указан в параметрах задачи).

Подключение к SMTP-серверу

В Kaspersky SIEM Cloud можно настроить отправку уведомлений по электронной почте с помощью SMTP-сервера. Пользователи будут получать уведомления, если в параметрах их профиля установлен флажок **Получать уведомления по почте**.

Для обработки уведомлений Kaspersky SIEM Cloud можно добавить только один SMTP-сервер. Управление подключением к SMTP-серверу осуществляется в Консоли OSMP в разделе **Параметры → KUMA → Открыть параметры KUMA → Общие → Параметры подключения к SMTP-серверу**.

Чтобы настроить подключение к SMTP-серверу:

1. В главном окне приложения перейдите в раздел **Параметры → KUMA → Открыть параметры KUMA**.
2. Откроется окно с параметрами Kaspersky SIEM Cloud.
3. В блоке **Другое** нажмите **Общие**.
4. Откроется окно **Общее**.
5. В блоке параметров **Параметры подключения к SMTP-серверу** измените необходимые параметры:
   - **Выключено** – установите этот флажок, если хотите отключить подключение к SMTP-серверу.
   - **Адрес сервера** (обязательно) – адрес SMTP-сервера в одном из следующих форматов: hostname, IPv4, IPv6.
   - **Порт** (обязательно) – порт подключения к почтовому серверу. Значение должно быть целым числом от 1 до 65 535.
   - **От кого** (обязательно) – адрес электронной почты отправителя сообщения. Например, `kuma@company.com`.

- **Псевдоним сервера Ядра KUMA** – название сервера Ядра Kaspersky SIEM Cloud, которое используется в вашей сети. Должно отличаться от полного доменного имени (FQDN).

- При необходимости в раскрывающемся списке **Секрет** выберите секрет типа **credentials**, в котором записаны учетные данные для подключения к SMTP-серверу.

  Добавить секрет

  Чтобы создать секрет:

  1. В поле **Название** введите название секрета.
  2. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору.
  3. При необходимости в поле **Описание** введите описание секрета.
  4. Нажмите на кнопку **Создать**.

  Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**.

- Выберите периодичность уведомлений в раскрывающемся списке **Регулярность уведомлений мониторинга**.

  Уведомления о срабатывании политики мониторинга от источника будут повторяться через выбранный период, пока статус источника не станет вновь зеленым.

  Если вы выберете значение **Не повторять**, уведомление о срабатывании политики мониторинга придет только один раз.

- Включите переключатель **Выключить уведомления мониторинга**, если не хотите получать уведомления о состоянии источников событий. По умолчанию переключатель выключен.

- Нажмите на кнопку **Проверить подключение**. Kaspersky SIEM Cloud отправит тестовое сообщение на адрес электронной почты, указанный в профиле текущего пользователя. Тестовое сообщение будет отправлено, даже если в профиле пользователя не установлен флажок **Получать уведомления по почте**.

  Проверьте ваш почтовый ящик. Если тестовое сообщение доставлено, SMTP-сервер настроен корректно. Если при отправке сообщения возникает ошибка, проверьте параметры SMTP-сервера. Ошибка отображается в интерфейсе, а также записывается в журнал Ядра Kaspersky SIEM Cloud. Если сообщение отправлено, но не доставлено в почтовый ящик, проверьте журнал SMTP-сервера на наличие сообщений об ошибках.

  Мы рекомендуем отправлять тестовое сообщение при каждом изменении параметров SMTP-сервера или шаблона уведомлений.

6. Нажмите на кнопку **Сохранить**.

Соединение с SMTP-сервером настроено, пользователи могут получать сообщения электронной почты от Kaspersky SIEM Cloud.

Изменение профиля пользователя

Чтобы изменить параметры профиля пользователя:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно с параметрами KUMA.

2. В разделе **Доступ** нажмите **Профиль**.

3. В правой части окна измените нужные параметры:

   - **Часовой пояс** – выберите часовой пояс, в котором будут отображаться временные метки при работе в Kaspersky SIEM Cloud. Список формируется на основе параметров операционной системы пользователя и учитывает переход на летнее и зимнее время. По умолчанию используется часовой пояс браузера пользователя.

   - **Использовать формат ISO 8601** – установите этот флажок, чтобы временные метки отображались в формате ISO 8601 (например, 2026-02-08T17:35:27+03:00). Формат применяется в тех разделах веб-интерфейса, где используется сокращенное или полное отображение даты и времени, и действует во всей системе Kaspersky SIEM Cloud. Настроенный формат сохраняется в параметрах Ядра Kaspersky SIEM Cloud.

   - **Получать уведомления по почте** – установите этот флажок, чтобы пользователь получал SMTP-уведомления от Kaspersky SIEM Cloud.

   - **Отображать непечатаемые символы** – установите этот флажок, чтобы в веб-интерфейсе Kaspersky SIEM Cloud отображались непечатаемые символы: пробелы, знаки табуляции, перенос на новую строку. Если флажок **Отображать непечатаемые символы** установлен, отображение непечатаемых символов можно включать и выключать, нажимая клавиши **`Ctrl/Command+*`**.

     Пробелы и знаки табуляции отображаются во всех полях ввода, кроме поля **Описание**, в ресурсах нормализаторов, правил корреляции, фильтров и коннекторов, а также в SQL-запросах на поиск событий в разделе **События**. Пробелы отображаются в виде точек. Знак табуляции отображается в виде тире в ресурсах нормализаторов, правил корреляции, фильтров и коннекторов. В других полях знак табуляции отображается в виде одной или двух точек.

     Символ переноса на новую строку отображается во всех полях ввода, поддерживающих многострочный ввод, например, в строке поиска событий.

   - В раскрывающемся списке **Наборы пространств** выберите один или несколько наборов пространств, к которым вы хотите предоставить доступ, установив рядом флажок. Если у пользователя нет выбранных наборов пространств, будет предоставлен доступ к набору пространств по умолчанию.

4. Нажмите **Сохранить**.

Профиль пользователя изменен.

Управление сертификатами

В этом разделе описана работа с сертификатами.

Скачивание сертификатов

В веб-консоли Kaspersky SIEM Cloud вы можете скачать следующие сертификаты:

- CA-сертификат REST API.

  Сертификат требуется для проверки подлинности API-сервера, обслуживающего публичное API Kaspersky SIEM Cloud. Также вы можете использовать этот сертификат при импорте данных из отчетов MaxPatrol.

  Сертификат можно изменить, если вы хотите использовать сертификат и ключ своей компании вместо самоподписанного сертификата веб-консоли.

  После загрузки сертификат можно импортировать в хранилище доверенных сертификатов операционной системы или браузера. После этого клиент будет доверять TLS-сертификату, который был выпущен Kaspersky SIEM Cloud и подписан удостоверяющим центром.

  Скачанный CA-сертификат не предназначен для редактирования. Если необходимо изменить список имен узлов (SAN) или использовать сертификат корпоративного удостоверяющего центра, следует выпустить новый TLS-сертификат и загрузить его в Kaspersky SIEM Cloud в разделе **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Общее** → **Параметры Ядра** → **Внешняя TLS-пара**.

  При установке в отказоустойчивой конфигурации в кластере Raft без использования балансировщика, вы можете скачать CA-сертификат REST API на любом узле, но защищенное соединение будет возможно только с узлом с core-1. На остальных узлах будет возвращаться ошибка. Если вы хотите заходить с одним сертификатом на все узлы кластера Raft напрямую без использования балансировщика, при генерации сертификата вы можете указать в поле `Subject Alternative Names` (SAN) FQDN всех узлов с сервисом Ядра Kaspersky SIEM Cloud в кластере Raft.

  Указание FQDN узлов в поле Subject Alternative Names (SAN) выполняется на этапе выпуска нового TLS-сертификата. Изменять скачанный CA-сертификат REST API не требуется.

  Если кластер содержит несколько узлов с сервисом Ядра Kaspersky SIEM Cloud и предполагается прямое подключение к каждому узлу, рекомендуется использовать TLS-сертификат, в SAN которого указаны FQDN всех узлов с сервисом Ядра Kaspersky SIEM Cloud. В противном случае браузер может отображать предупреждение о несоответствии имени узла сертификату.

- CA-сертификат микросервиса.

  Сертификат требуется для проверки подлинности при подключении источников журналов к пассивным коллекторам с использованием TLS, но без указания собственного сертификата.

- Сертификат AI-сервиса.

Чтобы скачать сертификат:

1. В веб-консоли перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**.
2. Установите флажок рядом с сервисом Ядра Kaspersky SIEM Cloud.
3. На панели инструментов в меню (⋮) выберите нужную опцию:
   - **Скачать CA-сертификат REST API**.
   - **Скачать CA-сертификат микросервиса**.
   - **Скачать сертификат AI-сервиса**.

Сертификат будет сохранен в папку, указанную в параметрах вашего браузера.

Чтобы скопировать отпечаток сертификата:

1. В веб-консоли перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**.
2. Установите флажок рядом с сервисом Ядра Kaspersky SIEM Cloud.
3. На панели инструментов в меню (⋮) выберите **Копировать отпечаток сертификата**.

   Идентификатор отпечатка сертификата скопирован в буфер обмена. Используйте идентификатор отпечатка CA-сертификата в качестве значения параметра `--pair.fingerprint` в команде установки сервиса для проверки подлинности сертификата Ядра Kaspersky SIEM Cloud при первом подключении сервиса к Ядру Kaspersky SIEM Cloud.

Изменение самоподписанного сертификата веб-консоли

Вы можете использовать сертификат и ключ своей компании вместо самоподписанного сертификата веб-консоли. Например, если вы хотите заменить сертификат веб-консоли с самоподписанного CA Core на сертификат, выпущенный корпоративным CA, необходимо предоставить `external.cert` и незашифрованный `external.key` в формате PEM.

В приведенной инструкции описано, как заменить самоподписанный CA Core с помощью корпоративного сертификата в формате PFX. Вы можете использовать инструкцию в качестве примера и адаптировать шаги в соответствии со своими потребностями.

Чтобы заменить сертификат веб-консоли Kaspersky SIEM Cloud на корпоративный сертификат в формате PFX:

1. Если вы используете сертификат и ключ в PFX-контейнере, в OpenSSL конвертируйте файл PFX в сертификат и зашифрованный ключ в формате PEM:

   ```
   openssl pkcs12 -in kumaWebIssuedByCorporateCA.pfx -nokeys -out external.cert
   ```

   ```
   openssl pkcs12 -in kumaWebIssuedByCorporateCA.pfx -nocerts -nodes -out external.key
   ```

   При выполнении команды потребуется указать пароль от ключа PFX (Enter Import Password).

   Вы получите сертификат `external.cert` и ключ `external.key` в формате PEM.

2. Если вы используете незашифрованный ключ `external.key`, убедитесь, что формат ключа – PKCS#8. Если файл ключа начинается с тега `BEGIN RSA PRIVATE KEY`, Kaspersky SIEM Cloud не сможет обработать файл ключа. В этом случае конвертируйте файл с помощью команды:

   ```
   openssl rsa -in rsa_private.key -outform PEM -out private.key
   ```

   После выполнения команды файл будет начинаться с тега `BEGIN PRIVATE KEY` и Kaspersky SIEM Cloud обработает файл ключа.

3. В веб-консоли откройте раздел **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Общее**.
4. В блоке параметров **Параметры Ядра** → **Внешняя TLS-пара** загрузите `external.cert` и незашифрованный `external.key` в формате PEM.

5. Перезапустите Kaspersky SIEM Cloud:

```
systemctl restart kuma-core
```

6. Обновите страницу или перезапустите браузер, с помощью которого вы работаете в веб-консоли.

Сертификат и ключ вашей компании заменены.

Перевыпуск внутренних CA-сертификатов

Перевыпускать внутренние CA-сертификаты могут только пользователи с ролью Главный администратор.

Чтобы перевыпустить и применить внутренние CA-сертификаты:

1. В веб-консоли откройте раздел **Параметры** → **KUMA** → **Открыть параметры KUMA** → **Общее** → **Параметры Ядра**.

2. В блоке **Внутренний CA-сертификат** нажмите на кнопку **Перевыпустить**.

3. В открывшемся окне подтвердите перевыпуск сертификата.

   CA-сертификаты для сервисов Kaspersky SIEM Cloud и CA-сертификат для ClickHouse будут перевыпущены. Перевыпущенные сертификаты требуется применить.

4. Подключитесь к хостам, на которых развернуты сервисы коллектора, коррелятора и маршрутизатора событий:

   a. Остановите все сервисы, выполнив команду:

   ```
   sudo systemctl stop kuma-<collector/correlator/eventRouter/metrics>-<service_ID>.service
   ```

   где:

   <service_ID> – идентификатор сервиса, скопированный из веб-консоли Kaspersky SIEM Cloud.

   b. Удалите файлы `internal.cert` и `internal.key` из директорий `/opt/kaspersky/kuma/<service_type>/<service_ID>/certificates`, выполнив следующие команды:

   ```
   sudo rm -f
   /opt/kaspersky/kuma/<collector/correlator/eventRouter/metrics>/<service_ID>/certificates/internal.cert
   sudo rm -f
   /opt/kaspersky/kuma/<collector/correlator/eventRouter/metrics>/<service_ID>/certificates/internal.key
   ```

5. Подключитесь к хостам, на которых развернуты сервисы хранилища:

   a. Остановите все сервисы хранилища:

   ```
   sudo systemctl stop kuma-<storage>-<service_ID>.service
   ```

b. Удалите файлы `internal.cert` и `internal.key` из директорий `/opt/kaspersky/kuma/storage/<service_ID>/certificates`, выполнив следующие команды:

```
sudo rm -f /opt/kaspersky/kuma/storage/<service_ID>/certificates/internal.cert
sudo rm -f /opt/kaspersky/kuma/storage/<service_ID>/certificates/internal.key
```

6. Удалите все сертификаты ClickHouse из директории `/opt/kaspersky/kuma/clickhouse/certificates`, выполнив следующие команды:

```
sudo rm -f /opt/kaspersky/kuma/clickhouse/certificates/internal.cert
```

```
sudo rm -f /opt/kaspersky/kuma/clickhouse/certificates/internal.key
```

7. Подключитесь к хостам, на которых развернуты сервисы агентов:

   a. Остановите сервисы агентов Windows и агентов Linux.

   b. Удалите файлы `internal.cert` и `internal.key` из рабочих директорий агентов.

8. Перезапустите Ядро Kaspersky SIEM Cloud, чтобы применить новые CA-сертификаты:

   - Для развертывания на одном сервере и распределенного развертывания выполните команду:

     ```
     sudo systemctl restart kuma-core-00000000-0000-0000-0000-000000000000.service
     ```

   - Для развертывания в кластере Kubernetes, на любом контроллере выполните следующие команды:

     ```
     sudo k0s kubectl exec deployment/metrics -n kuma -- rm -rf /opt/kaspersky/kuma/metrics/certificates
     sudo k0s kubectl rollout restart deployment metrics -n kuma
     sudo k0s kubectl rollout restart deployment/core-deployment -n kuma
     ```

     Рекомендуется перезапускать Ядро Kaspersky SIEM Cloud с помощью команды, поскольку перезапуск через веб-консоль влияет на перезапуск только контейнера Ядра Kaspersky SIEM Cloud, а не весь под целиком.

9. Перейдите в раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**, установите флажок рядом с сервисом Ядра Kaspersky SIEM Cloud.

10. На панели инструментов в меню (⋮) выберите **Копировать отпечаток сертификата**.

    Отпечаток CA-сертификата Ядра Kaspersky SIEM Cloud скопирован в буфер обмена.

11. На каждом хосте, где установлены сервисы Kaspersky SIEM Cloud, вставьте скопированный отпечаток в качестве значения параметра `--pair.fingerprint` в файле systemd сервиса.

12. Выполните следующую команду, чтобы применить изменения в файле systemd:

```
sudo systemctl daemon-reload
```

13. Перезапустите все остановленные сервисы:

```
sudo systemctl start kuma-<collector/correlator/eventRouter/storage/metrics>-<service_ID>.service
```

где:

<service_ID> — идентификатор сервиса, скопированный из веб-консоли Kaspersky SIEM Cloud.

Новые внутренние CA-сертификаты будут применены.

Перевыпуск сертификата для отдельного сервиса

Чтобы сбросить сертификат для отдельного сервиса:

1. В веб-консоли откройте раздел **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**.
2. Установите флажок рядом с тем сервисом, сертификат которого вы хотите перевыпустить.
3. В панели инструментов или в меню ⋮ выберите **Сбросить сертификат**.

   Этот вариант недопустимо использовать для обновления сертификата Ядра Kaspersky SIEM Cloud. Чтобы обновить сертификаты Ядра Kaspersky SIEM Cloud, их требуется перевыпустить и применить внутренние CA-сертификаты.

4. Удалите прежний сертификат в директории установки сервиса.

   Решение автоматически сгенерирует новый сертификат. Для работающих сервисов перезапуск не требуется, новый сертификат будет применен автоматически. Если сервис был остановлен, необходимо перезапустить сервис, чтобы применить новый сертификат.

Особенности удаления сертификатов для агентов Windows:

- Если агент находится в зеленом статусе, Kaspersky SIEM Cloud удаляет действующий сертификат и создает новый. Агент продолжит работу с новым сертификатом.
- Если агент находится в красном статусе, отображается ошибка, что агент не запущен. В папке установки агента `%PROGRAMDATA%\Kaspersky Lab\KUMA\agent\<agent_ID>\certificates` следует удалить файлы `internal.cert` и `internal.key` и вручную запустить агент. При запуске агента новый сертификат будет создан автоматически.

Особенности удаления сертификатов для агентов Linux:

- Независимо от статуса агента сертификат сбрасывается через веб-консоль.
- В папке установки агента `/opt/kaspersky/agent/<ID агента>/certificates` нужно удалить файлы `internal.cert` и `internal.key`.
- Поскольку при сбросе сертификата работа агента будет остановлена, для продолжения работы нужно вручную запустить агент. При запуске агента новый сертификат создается автоматически.

Интеграция с другими решениями

Интеграция с другими решениями позволяет расширить функциональность Kaspersky SIEM Cloud.

Kaspersky Automated Security Awareness Platform

Kaspersky Automated Security Awareness Platform (далее также "KASAP") – это платформа для онлайн-обучения, с помощью которой пользователи смогут усвоить правила соблюдения информационной безопасности, узнать о связанных с ней угрозах, подстерегающих их в ежедневной деятельности, и потренироваться на практических примерах.

Платформу KASAP можно интегрировать с KUMA. После настройки интеграции в KUMA можно выполнять следующие задачи:

- Изменять группы обучения пользователей.
- Просматривать информацию о курсах, пройденных пользователями, и полученных ими сертификатах.

Интеграция KASAP и KUMA заключается в настройке API-подключения к платформе KASAP. Процесс происходит в обоих продуктах:

1. В KASAP необходимо создать токен для авторизации API-запросов и получить адрес для API-запросов.
2. В KUMA необходимо указать адрес для API-запросов в KASAP, добавить токен для авторизации API-запросов, а также указать адрес электронной почты администратора KASAP для получения уведомлений.

Создание токена в KASAP и получение ссылки для API-запросов

Для авторизации API-запросов из KUMA в KASAP их необходимо подписывать токеном, созданном в платформе KASAP. Только администраторы компании могут создать токены.

Создание токена

Чтобы создать токен:

1. Войдите в веб-интерфейс KASAP.
2. В разделе **Контрольная панель** нажмите на кнопку **Импорт и синхронизация**, а затем откройте вкладку **Open API**.

3. Нажмите на кнопку **Новый токен** и в открывшемся окне выберите методы API, используемые при интеграции:

   - GET /openapi/v1/groups
   - POST /openapi/v1/report
   - PATCH /openapi/v1/user/:userid

4. Нажмите на кнопку **Сгенерировать токен**.

5. Скопируйте токен и сохраните его любым удобным способом. Этот токен необходим для настройки интеграции в KUMA.

> Токен не хранится в системе KASAP в открытом виде. После закрытия окна **Получить токен** он становится недоступным для просмотра. Если вы закрыли это окно, не скопировав токен, вам требуется нажать на кнопку **Новый токен** повторно, чтобы система сгенерировала новый токен.

Выданный токен действителен 12 месяцев. По истечении этого срока токен будет отозван. Выпущенный токен будет также отозван, если он не используется в течении 6 месяцев.

Получение ссылки для API-запросов

Чтобы получить ссылку, используемую в KASAP для API-запросов:

1. Войдите в консоль платформы KASAP.

2. В разделе **Контрольная панель** нажмите на кнопку **Импорт и синхронизация**, а затем откройте вкладку **Open API**.

3. Ссылка для обращения к KASAP через Open API расположена в нижней части окна. Скопируйте ссылку и сохраните ее любым удобным способом. Эта ссылка необходима для настройки интеграции в KUMA.

Настройка интеграции в KUMA

Чтобы настроить в KUMA интеграцию с KASAP:

1. В главном окне приложения перейдите в раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.

   Откроется окно **Параметры KUMA**.

2. В разделе **Интеграции** нажмите **Kaspersky Automated Security Awareness Platform**.

   Откроется окно **Интеграция с Kaspersky Automated Security Awareness Platform**.

3. В поле **Секрет** с помощью значка плюса (+) создайте секрет типа **token**, указав в нем токен, полученный в платформе KASAP:

   a. В поле **Название** введите название для секрета. Имя должно содержать от 1 до 128 символов Юникода.

   b. В поле **Токен** введите токен для авторизации API-запросов в KASAP.

c. При необходимости добавьте описание секрета в поле **Описание**.

d. Нажмите на кнопку **Сохранить**.

4. В поле **URL для OpenAPI KASAP** укажите адрес, используемый платформой KASAP для API-запросов.

5. В поле **Адрес электронной почты администратора KASAP** укажите адрес электронной почты администратора KASAP, который должен получать уведомления при добавлении пользователей в группы обучения через KUMA.

6. При необходимости в раскрывающемся списке **Прокси-сервер** выберите ресурс прокси-сервера, который следует использовать для подключения к платформе KASAP.

7. При необходимости выключить или включить интеграцию с KASAP установите или снимите флажок **Выключено**.

8. Нажмите на кнопку **Сохранить**.

В KUMA настроена интеграция с KASAP. Теперь при просмотре информации об алертах и инцидентах можно выбрать относящихся к ним пользователей, чтобы просмотреть, какие курсы обучения прошли пользователи, а также изменить их группу обучения.

Просмотр данных о пользователях KASAP и изменение учебных групп

После настройки интеграции KASAP и KUMA в алертах и инцидентах при просмотре данных о связанных с ними пользователях становятся доступны данные из KASAP:

- Учебная группа, к которой принадлежит пользователь.
- Сведения о пройденных курсах.
- Сведения о запланированном обучении и текущем прогрессе.
- Сведения о полученных сертификатах.

Чтобы просмотреть данные о пользователе из KASAP:

1. В Консоли OSMP в разделе **Алерты** или **Инциденты** выберите нужный алерт или инцидент.

2. В разделе **Связанные пользователи** нажмите на нужную учетную запись.

   В правой части экрана откроется окно **Информация об учетной записи**.

3. Выберите вкладку **Данные о курсах KASAP**.

В окне отображаются данные пользователя из KASAP.

Вы можете изменить учебную группу пользователя KASAP.

Чтобы изменить учебную группу KASAP:

1. В Консоли OSMP в разделе **Алерты** или **Инциденты** выберите нужный алерт или инцидент.
2. В разделе **Связанные пользователи** нажмите на нужную учетную запись.

   В правой части экрана откроется окно **Информация об учетной записи**.
3. В раскрывающемся списке **Присвоить пользователю группу KASAP** выберите учебную группу KASAP, в которую вы хотите поместить пользователя.
4. Нажмите **Применить**.

Пользователь будет перемещен в выбранную группу KASAP, администратор компании платформы KASAP получит уведомление об изменении состава учебных групп, а для выбранной учебной группы начнет пересчитываться учебный план.

Подробнее об учебных группах и начале обучения см. в документации KASAP.

Мониторинг и отчеты

В этом разделе описаны функции мониторинга и работа с отчетами в Kaspersky SIEM Cloud. Эти функции позволяют получать сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.

В процессе развертывания или во время работы Kaspersky SIEM Cloud можно настраивать функции мониторинга и параметры отчетов.

Сценарий: мониторинг и отчеты

В этом разделе представлен сценарий настройки мониторинга и отчетов в Kaspersky SIEM Cloud.

Предварительные требования

После развертывания Kaspersky SIEM Cloud в сети организации вы можете приступить к мониторингу состояния безопасности сети с помощью Kaspersky Security Center и к формированию отчетов.

Мониторинг и работа с отчетами в сети организации состоят из следующих этапов:

1. **Настройка переключения статусов устройств**

   Ознакомьтесь с параметрами статусов устройства в зависимости от конкретных условий. Изменяя эти параметры, вы можете изменить количество событий с уровнями важности *Критический* или *Предупреждение*. При настройке переключения состояний устройства убедитесь, что:

   - новые параметры не противоречат политикам информационной безопасности вашей организации;
   - вы можете своевременно реагировать на важные события безопасности в сети вашей организации.

2. **Настройка параметров уведомлений о событиях на клиентских устройствах**

   Инструкции:

   Настройка уведомлений (по электронной почте, по SMS или с помощью запуска исполняемого файла) о событиях на клиентских устройствах.

3. **Выполнение рекомендуемых действий для критических и предупреждающих уведомлений**

   Инструкции:

   Выполните рекомендуемые действия для сети вашей организации.

4. **Просмотр состояния безопасности сети вашей организации**

   Инструкции:

   - Просмотр виджета Состояние защиты.
   - Генерация и просмотр отчета Отчет о состоянии защиты.
   - Генерация и просмотр отчета Отчет об ошибках.

5. **Нахождение незащищенных клиентских устройств**

   Инструкции:

   - Просмотр виджета Новые устройства.
   - Генерация и просмотр отчета Отчет о развертывании защиты.

6. **Проверка защиты клиентских устройств**

   Инструкции:

   - Генерация и просмотр отчета из категорий Состояние защиты и Статистика угроз.
   - Запуск и просмотр выборки событий Критическое.

7. **Оценка и ограничение загрузки событий в базу данных**

   Информация о событиях, которые возникают во время работы управляемых приложений, передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

   Инструкции:

   - Ограничение максимального количества событий.

8. **Просмотр информации о лицензии**

   Инструкции:

   - Добавление виджета Используемые лицензионные ключи в панель мониторинга и его просмотр.
   - Генерация и просмотр отчета Отчет об использовании лицензионных ключей.

Результаты

После завершения сценария вы будете проинформированы о защите сети вашей организации и, таким образом, сможете планировать действия для дальнейшей защиты.

О типах мониторинга и отчетах

Информация о событиях безопасности в сети организации хранится в базе данных Сервера администрирования. OSMP Console предоставляет следующие виды мониторинга и отчетов в сети вашей организации:

- Панель мониторинга
- Отчеты
- Выборки событий
- Уведомления

Панель мониторинга

Панель мониторинга позволяет контролировать состояние безопасности в сети вашей организации с помощью графического представления информации.

Отчеты

Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

Выборки событий

Выборки событий предназначены для просмотра на экране именованных наборов событий, которые выбраны из базы данных Сервера администрирования. Эти типы событий сгруппированы по следующим категориям:

- Уровень важности: **Критические события**, **Отказы функционирования**, **Предупреждения** и **Информационные события**.
- Время: **Последние события**.
- Тип: **Запросы пользователей** и **События аудита**.

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе OSMP Console.

Уведомления

Уведомления предназначены для оповещения о событиях и для того, чтобы помочь вам увеличить скорость ваших ответов на эти события, выполнив рекомендуемые действия, которые вы считаете подходящими.

Панель мониторинга и виджеты

В этом разделе содержится информация о панели мониторинга и виджетах, представленных в панели мониторинга. Раздел содержит инструкции по управлению виджетами и настройке виджетов.

Использование панели мониторинга

Панель мониторинга позволяет контролировать состояние безопасности в сети вашей организации с помощью графического представления информации.

Панель мониторинга доступна в OSMP Console: в разделе **Мониторинг → Панель мониторинга**.

В панели мониторинга представлены настраиваемые виджеты. Вы можете выбрать большое количество различных виджетов, представленных в виде круговых диаграмм, таблиц, графиков, гистограмм и списков. Информация, отображаемая в виджетах, обновляется автоматически, период обновления составляет от одной до двух минут. Интервал времени между обновлениями зависит от типа виджета. Вы можете обновить данные виджета вручную с помощью меню в любое время.

Панель управления включает в себя вкладки **Панель мониторинга** и **Обнаружение и реагирование**, на которые вы можете добавлять виджеты.

Вкладка Панель мониторинга

Вкладка **Панель мониторинга** может содержать виджеты, которые отображают информацию о всех событиях, хранящихся в базе данных Сервера администрирования.

На вкладке **Панель мониторинга** доступны виджеты следующих категорий:

- **Состояние защиты**
- **Развертывание**
- **Обновление**
- **Обновление приложений**
- **Статистика угроз**
- **Другие**

Вкладка Обнаружение и реагирование

Вкладка **Обнаружение и реагирование** может содержать виджеты, которые отображают информацию о зарегистрированных алертах и инцидентах, а также действиях по реагированию на них. Вы можете просматривать данные только для тех тенантов, к которым у вас есть доступ.

На вкладке **Обнаружение и реагирование** доступны виджеты следующих категорий:

- **События**
- **Активные листы**
- **Контекстные таблицы**
- **Активы**
- **Алерты**
- **Инциденты**
- **Источники событий**
- **Пользователи**
- **Плейбуки**
- **Правила**
- **Изображение**
- **Текст**

Виджеты администрирования и защиты

При настройке вкладки **Панель мониторинга** можно добавлять виджеты, скрывать виджеты, а также менять внешний вид или размер виджетов, перемещать виджеты и изменять параметры виджетов.

Некоторые виджеты имеют текст со ссылками. Чтобы просмотреть подробную информацию, перейдите по ссылке.

На вкладке **Панель мониторинга** доступны следующие категории виджетов и виджеты:

- **Состояние защиты**

  В группу входят следующие виджеты:

  - **История наличия экземпляров уязвимостей в приложениях**
  - **Количество уязвимых устройств**
  - **Количество устройств**

- **Статусы выбранных устройств**
- **Состояние защиты**

- **Развертывание.**

  Эта группа включает в себя виджет **Новые устройства**.

- **Обновление.**

  Эта группа включает следующие виджеты:

  - **Статистика проверки обновлений Центра обновления Windows**
  - **Распространение антивирусных баз**

- **Обновление приложений.**

  Эта группа включает следующие виджеты:

  - **Статистика результатов установки обновлений по категории обновления**
  - **Статистика состояния установки обновлений по категории обновления**
  - **Статистика состояния установки обновлений**

- **Статистика угроз.**

  Эта группа включает следующие виджеты:

  - **Обнаружение угроз с помощью указанного компонента приложения, отсортированных по результатам их лечения**
  - **Обнаружение угроз компонентами приложения**
  - **Запрещенные приложения**
  - **Типы сетевых атак**
  - **Типы обнаруженных вирусов и результаты лечения**
  - **История помещения файлов на карантин**
  - **История обнаружения возможно зараженных объектов**
  - **История сетевых атак**
  - **История активности угроз по типам приложений**
  - **Активность угроз**
  - **Пользователи 10 наиболее зараженных устройств**
  - **Наиболее зараженные устройства**
  - **Самые заражаемые виртуальные Серверы**
  - **Наиболее распространенные угрозы**

- **Наиболее заражаемые Windows-домены**
- **Наиболее заражаемые группы**
- **Алерты**

- **Другие**

  Эта группа включает следующие виджеты:

  - **Cloud Discovery**
  - **Используемые лицензионные ключи**
  - **Десять наиболее частых событий базы данных**
  - **Текущее состояние выбранной задачи Сервера администрирования**
  - **История задачи**

Добавление виджета на информационную панель

Чтобы добавить виджет на информационную панель:

1. В веб-консоли перейдите в раздел **Мониторинг** → **Панель мониторинга**.
2. Нажмите на кнопку **Добавить или восстановить виджет**.
3. В списке доступных виджетов выберите виджет, который требуется добавить на информационную панель.

   Виджеты сгруппированы по категориям. Чтобы посмотреть, какие виджеты входят в категорию, нажмите на значок шеврона (>) рядом с именем категории.
4. Нажмите на кнопку **Добавить**.

Выбранные виджеты будут добавлены в конец информационной панели.

Можно изменить внешний вид и параметры добавленных виджетов.

Удаление виджета с информационной панели

Чтобы удалить виджет с информационной панели:

1. В веб-консоли перейдите в раздел **Мониторинг** → **Панель мониторинга**.
2. Нажмите на значок меню (⋮) рядом с виджетом, который нужно удалить.
3. Выберите **Скрыть виджет**.
4. В появившемся окне **Предупреждение** нажмите на кнопку **ОК**.

Выбранный виджет будет удален с информационной панели. В дальнейшем можно опять добавить виджет на информационную панель.

Перемещение виджета на информационной панели

Чтобы переместить виджет на информационной панели:

1. В веб-консоли перейдите в раздел **Мониторинг → Панель мониторинга**.
2. Нажмите на значок меню (⋮) рядом с виджетом, который нужно переместить.
3. Выберите **Переместить**.
4. Укажите место, куда требуется переместить виджет. Можно выбрать только другой виджет.

Выбранные виджеты поменяются местами.

Изменение размера или внешнего вида виджета

Можно изменить внешний вид виджетов: выбрать столбчатую или линейную диаграмму. Для некоторых виджетов можно изменить размер: маленький, средний или крупный.

Чтобы изменить внешний вид виджета:

1. В веб-консоли перейдите в раздел **Мониторинг → Панель мониторинга**.
2. Нажмите на значок меню (⋮) рядом с виджетом, который нужно изменить.
3. Выполните одно из следующих действий:
   - Чтобы виджет отображался как столбчатая диаграмма, выберите **Тип диаграммы: линейчатая диаграмма**.
   - Чтобы виджет отображался как линейная диаграмма, выберите **Тип диаграммы: линейный график**.
   - Чтобы поменять размер области, занимаемой виджетом, выберите одно из значений:
     - **Минимальный**
     - **Минимальный (только линейчатая диаграмма)**
     - **Средний (кольцевой график)**
     - **Средний (линейчатая диаграмма)**
     - **Максимальный**

Внешний вид выбранного виджета будет изменен.

Изменение параметров виджета

Чтобы изменить параметры виджета:

1. В веб-консоли перейдите в раздел **Мониторинг → Панель мониторинга**.
2. Нажмите на значок меню (⋮) рядом с виджетом, который нужноизменить.
3. Выберите **Показать параметры**.

4. В открывшемся окне параметров виджета измените нужные параметры виджета.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Параметры выбранного виджета будут изменены.

Набор параметров зависит от конкретного виджета. Ниже приведены некоторые общие параметры:

- **Область виджета** – набор объектов, для которых виджет отображает информацию; например, группа администрирования или выборка устройств.
- **Выберите задачу** – задача, для которой виджет отображает информацию.
- **Период** – период, за который отображается информация в виджете; например, между двумя заданными датами, от заданной даты до настоящего времени или за указанное количество дней до настоящего времени.
- **Установить статус "Критический", если** и **Установить статус "Предупреждение", если** – правила, в соответствии с которыми назначаются цвета на графике статусов.

После изменения параметров виджета вы можете обновить данные виджета вручную.

Чтобы обновить данные виджета:

1. В веб-консоли перейдите в раздел **Мониторинг → Панель мониторинга**.
2. Нажмите на значок меню (⋮) рядом с виджетом, который нужно обновить.
3. Нажмите на кнопку **Обновить**.

Данные виджета обновлены.

Веб-виджеты обнаружения и реагирования

На вкладке **Обнаружение и реагирование** вы можете добавлять, настраивать и удалять виджеты.

Набор виджетов, используемых на вкладке **Обнаружение и реагирование**, называется *макетом*. Все веб-виджеты должны быть размещены на макетах. Kaspersky SIEM Cloud позволяет создавать, изменять и удалять макеты. Также доступны преднастроенные макеты панели мониторинга. При необходимости вы можете изменять параметры виджета в предварительно настроенных макетах. По умолчанию на вкладке **Обнаружение и реагирование** выбран макет **Обзор алертов**.

Перейдя по ссылке с названием виджета о событиях, алертах, инцидентах или активных листах, вы можете перейти в соответствующий раздел интерфейса Kaspersky SIEM Cloud. Обратите внимание, что этот параметр недоступен для некоторых виджетов.

На вкладке **Обнаружение и реагирование** в панели мониторинга доступны следующие категории виджетов и виджеты:

- **События**. Виджет для создания аналитики на основе событий.
- **Активные листы**. Виджет для создания аналитики на основе активных листов корреляторов.
- **Контекстные таблицы**. Виджет для создания аналитики на основе контекстных таблиц.

- **Алерты**. Группа для аналитиков, которые работают с алертами. Включает информацию об алертах и инцидентах, предоставляемую Kaspersky SIEM Cloud.

  В группу входят следующие веб-виджеты:

  - **Активные алерты**. Количество незакрытых алертов.
  - **Неназначенные алерты**. Количество алертов, у которых нет исполнителя.
  - **Активные алерты по тенантам**. Количество незакрытых алертов, сгруппированных по тенантам.
  - **Алерты по хешу файла**. Количество алертов, сгруппированных по хешам проверенных объектов. Поддерживаемые типы хешей: MD5 и SHA256.
  - **Алерты по тенантам**. Количество алертов, сгруппированных по тенантам.
  - **Алерты по пользователям**. Количество алертов со статусом *Назначен*. Сгруппированы по имени учетной записи.
  - **Алерты по группам**. Количество алертов, назначенных каждой группе и аналитикам в каждой группе. Алерты, назначенные аналитику, учитываются в каждой группе, членом которой является этот аналитик.
  - **Алерты по статусу**. Количество алертов со статусами *Новый*, *Открыт*, *Назначен* или *Эскалирован*. Сгруппированы по статусу.
  - **Алертов по уровню важности**. Количество незавершенных алертов, сгруппированных по уровню важности.
  - **Алерты по правилу корреляции**. Количество незакрытых алертов, сгруппированных по правилу корреляции.
  - **Последние алерты**. Таблица с информацией о последних 10 незакрытых алертах.
  - **Распределение алертов**. Количество алертов, созданных в течение указанного для виджета периода.
  - **Распределение алертов по статусам (статусы алертов за период)**. Количество алертов по статусу за выбранный период.
  - **Распределение алертов по уровню важности**. Количество алертов по уровню важности за выбранный период
  - **Распределение алертов по технологиям**. Количество алертов по технологиям за выбранный период.
  - **Алерты по технологиям**. Название технологии для защиты, в результате проверки которой был создан алерт.
  - **Алерты по источнику обнаружения**. Количество алертов, сгруппированных по источнику обнаружения.
  - **Алерты по имени файла**. Количество алертов, сгруппированных по имени проверяемого файла.
  - **Настраиваемая таблица алертов**.

- **Активы**. Группа для аналитики об активах из обработанных событий.

Эта группа включает следующие виджеты:

- **Пользовательский виджет**.
- **Активы из KSC**. Таблица с информацией об активах из KSC.
  - **Статусы активов из KSC**.
  - **Тенанты активов из KSC с уязвимостями**.
  - **Время загрузки или обновления активов из KSC**.
  - **Статус постоянной защиты активов из KSC**.
  - **Расширенный статус постоянной защиты активов из KSC**.
- **Затронутые активы**. Таблица с информацией об активах и количестве незакрытых алертов, которые связаны с этими активами. Переход от виджета к разделу со списком активов недоступен.
- **Категории затронутых активов**. Категории активов, привязанных к незакрытым алертам.
- **Количество активов**. Количество активов, добавленных в Kaspersky SIEM Cloud.
- **Активы в инцидентах по тенантам**. Количество активов, связанных с незакрытыми инцидентами. Сгруппированы по тенантам.
- **Активы в алертах по тенантам**. Количество активов, связанных с незакрытыми алертами, Сгруппированы по тенантам.

- **Инциденты**. Группа для аналитиков, которые работают с инцидентами.

  В группу входят следующие виджеты:

  - **Активные инциденты**. Количество незакрытых инцидентов.
  - **Неназначенные инциденты**. Количество инцидентов со статусом *Открыт*.
  - **Инцидентов по уровню важности**. Количество незавершенных инцидентов, сгруппированных по уровню важности.
  - **Активные инциденты по тенантам**. Количество незакрытых инцидентов, сгруппированных по тенантам.
  - **Категории активов в инцидентах**. Категории активов, которые затронуты незакрытыми инцидентами.
  - **Пользователи в инцидентах**. Количество пользователей, связанных с инцидентами. Переход от виджета к разделу со списком пользователей недоступен
  - **Распределение инцидентов**. Количество инцидентов, созданных в течение указанного для виджета периода.
  - **Инциденты по пользователям**. Количество инцидентов со статусом *Назначен*. Сгруппированы по имени учетной записи пользователя.
  - **Инциденты по группам**. Количество инцидентов, назначенных каждой группе и аналитикам в каждой группе. Инциденты, назначенные аналитику, учитываются в каждой группе, членом которой является этот аналитик.

- **Инциденты по статусам**. Количество инцидентов, сгруппированных по статусам.
- **Все инциденты**. Количество инцидентов всех статусов.
- **Все инциденты по тенантам**. Количество инцидентов всех статусов, сгруппированных по тенантам.
- **Активы в инцидентах**. Количество активов в незакрытых инцидентах. Переход от виджета к разделу со списком активов недоступен
- **Последние инциденты**. Таблица с информацией о последних 10 незакрытых инцидентах.
- **Инцидентов по типу**. Количество инцидентов в любом статусе, сгруппированных по типу.

- **Источники событий**. Группа для аналитиков, которые работают с событиями. В группу входят следующие виджеты:
  - **Топ источников событий (значение в поле DeviceProduct) по количеству базовых событий, собранных в корреляционных событиях** – количество базовых событий, собранных в корреляционных событиях и сгруппированных по источникам данных, указанным в поле `DeviceProduct`.
  - **Топ источников событий (значение в поле DeviceProduct) по условному рейтингу** – соотношение между числом базовых событий в корреляционных событиях и общим числом базовых событий, сгруппированных по источникам данных, указанным в поле `DeviceProduct`.

    В ряде случаев количество корреляционных событий, созданных источниками, может быть искажено. Для получения точной статистики рекомендуется в правиле корреляции указать поле события `Device Product` в качестве уникального, а также включить хранение всех базовых событий в корреляционном событии. Правила корреляции с такими параметрами являются более ресурсоемкими.

- **Пользователи**. Группа для аналитики о пользователях из обработанных событий. В группу входят следующие виджеты:
  - **Пользователи в алертах**. Количество учетных записей, связанных с незакрытыми алертами.
  - **Количество пользователей AD**. Количество учетных записей в Active Directory, полученных по LDAP в течение указанного в виджете периода.

    В таблице событий, в области сведений о событиях, в окне алертов и в виджетах имена активов, учетных записей и служб отображаются вместо идентификаторов в качестве значений полей `SourceAssetID`, `DestinationAssetID`, `DeviceAssetID`, `SourceAccountID`, `DestinationAccountID` и `ServiceID`. При экспорте событий в файл идентификаторы сохраняются, но в файл добавляются столбцы с именами. Идентификаторы также отображаются при наведении курсора мыши на названия активов, учетных записей или служб.
    Поиск полей с идентификаторами возможен только по идентификаторам.

- **Плейбуки**. Группа для аналитиков, которые работают с плейбуками.

Для просмотра виджетов в этой группе у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Администратор SOC, Менеджер SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Подтверждающий, Аудитор.

В группу входят следующие виджеты:

- **Статистика MTTR**. Изменение времени первого действия по реагированию на алерты и инциденты за указанный период времени (по умолчанию 30 дней). Виджет отображает столбчатую диаграмму.

  Доступны следующие параметры конфигурации виджета **Статистика MTTR**:

  - **Тип MTTR**:

    - **Значение**. Изменяет среднее время до первого действия по реагированию на алерт и инциденты.

    - **Минимальный**. Изменяет минимальное время до первого действия по реагированию на алерты и инциденты.

    - **Максимальный**. Изменяет максимальное время до первого действия по реагированию на алерты и инциденты.

  - **Режим реагирования**:

    - **Вручную**. Изменяет время только для первых действий по реагированию вручную.

    - **Автоматически**. Изменяет время только для автоматических первых действий по реагированию.

    - **Все**. Изменяет время на все первые действия по реагированию.

  - **Область действия**:

    - **Алерты**. Изменяет время до первого действия по реагированию только на алерты.

    - **Инциденты**. Изменяет время до первого действия по реагированию только на инциденты.

    - **Все**. Изменяет время до первого действия по реагированию на алерты и инциденты.

- **Автоматические и ручные запуски плейбуков**. Общее количество автоматических и ручных запусков плейбуков за определенный период. Виджет отображает столбчатую диаграмму.

  Параметр **Тип запуска** для виджета указывает, следует ли отображать только количество автоматических запусков, только запусков вручную или общее количество запусков плейбуков за определенный период.

  Для виджетов **Статистика MTTR** и **Автоматический и ручной запуск плейбуков** вы также можете установить параметр **Длина сегментов периода**. Этот параметр указывает период, в течение которого будут сгруппированы данные. Вы можете группировать данные за каждый час, каждые 4 часа или каждые 24 часа. На столбчатой диаграмме параметр **Длина сегментов периода** указывает ширину столбца.

- **Покрытие плейбуками алертов и инцидентов**. Количество активных алертов и инцидентов. Вы можете выбрать, какие компоненты отображать: инциденты, алерты или все.

  На кольцевой диаграмме отображаются алерты/инциденты в следующих секторах:

  - Алерты/инциденты, для которых был запущен плейбук в режиме **Автоматический**.

  - Алерты/инциденты, для которых был запущен плейбук в режиме **Обучение**.

  - Все остальные алерты/инциденты.

- **Суммарное сэкономленное время за счет использования плейбуков**. Экономия времени за счет запуска всех плейбуков со *статусом Успешно* или Предупреждение.

  По умолчанию виджет не отображается.

Вы можете просмотреть полный список плейбуков, нажав на имя любого виджета плейбука.

- **Правила**. Группа для аналитиков, которые работают с правилами.

  В группу входят следующие виджеты:

  - **Топ 10 IOA-правил, инициировавших сканирование Sandbox**. Топ 10 IOA-правил, по которым Kaspersky Anti Targeted Attack Platform наиболее часто передает файлы на проверку компоненту Sandbox.
  - **Топ 10 срабатывающих IOA-правил**. Топ 10 IOA-правил, наиболее часто срабатывающих в событиях и алертах, обнаруженных технологией Targeted Attack Analyzer (TAA).
  - **Топ 10 хостов со срабатыванием IOA**. Топ-10 устройств, на которых IOA-правила срабатывали чаще всего.

- **Изображение**. Виджет для отображения загруженного изображения на панели мониторинга или в отчете.
- **Текст**. Виджет для отображения произвольного текста на панели мониторинга или в отчете.

Основные принципы работы с виджетами

Принцип отображения данных на веб-виджете зависит от типа графика. В Kaspersky SIEM Cloud доступны следующие типы графиков:

- Круговая диаграмма ( ).
- Счетчик ( ).
- Таблица ( ).
- Столбчатая диаграмма ( ).
- Календарная диаграмма ( ).
- Линейная диаграмма.
- Сложенная столбчатая диаграмма.
- Спидометр.

Основные принципы работы со всеми виджетами

В левом верхнем углу виджетов отображается название виджета. По ссылке с названием виджета о событиях, алертах, инцидентах или активных листах вы можете перейти в соответствующий раздел OSMP Console.

Под названием виджета отображается список тенантов, для которых представлены данные.

В правом верхнем углу виджета указан период, за который отображаются данные на виджете (например, 30 дней 30д). При этом данные, отображающиеся в панели мониторинга, могут отставать от реального времени, так как они сохраняются в кеш. Вы можете просмотреть дату и время последнего обновления, наведя курсор на значок периода.

Если параметр **Показать данные за предыдущий период** включен в свойствах виджета и виджет отображает данные за относительный период, во всплывающей подсказке также отображается предыдущий период. Предыдущий период рассчитывается относительно текущего периода – из начального и конечного значения текущего периода вычитается продолжительности текущего периода. Например, если данные обновляются ежедневно и отображаются за месяц, но прошли только первые 10 дней месяца, прошлым периодом будут считаться последние 10 дней прошлого месяца.

Вы можете изменить период отображения данных на виджете, нажав на значок периода и выбрав точную дату или относительный период в открывшемся окне. Если вы хотите отобразить на виджете данные за период, выбранный для макета, вы можете нажать на кнопку **Сбросить**. При изменении периода отображения данных на макете, также изменится отображаемый на виджете период.

Время на виджете приводится в соответствие с локальным часовым поясом, установленном в браузере.

Слева от значка периода отображается кнопка **CSV**. Вы можете скачать данные, которые отображаются на виджете, в формате CSV (кодировка UTF-8). Имя скачиваемого файла имеет формат <название виджета>_<дата скачивания (ГГГГММДД)>_<время скачивания (ЧЧММСС)>.CSV.

виджет отображает данные за период, выбранный в параметрах виджета или макета, только для тенантов, указанных в параметрах виджета или макета.

Если вы при настройке виджета включили переключатель **Итоговые значения**, на виджете отображается значение **Всего**, но при выгрузке виджета в формате CSV значение **Всего** не отображается. Для отображения значения **Всего** в отчете, вы можете воспользоваться формулами Excel или переписать итоговое значение с виджета.

Основные принципы работы с графиками типа Круговая диаграмма

Под списком тенантов отображается круговая диаграмма с легендой. В легенде отображаются названия категорий, соответствующих секторам диаграммы. Из контекстного меню категории в легенде можно перейти в раздел OSMP Console с соответствующими данными. Данные в разделе будут отсортированы в соответствии с фильтрами и/или поисковым запросом, указанным в виджете.

При переходе из легенды виджета в раздел событий для детализации информации обратите внимание на текст элемента легенды, по которому вы переходите в раздел событий. Если в тексте используется символы \ или ', то они будут экранированы в тексте SQL-запроса. При этом символ / не экранируется.

Под значком периода отображается количество событий, активных листов, активов, алертов или инцидентов, сгруппированных по выбранным критериям за период отображения данных на виджетах.

Примеры:

- На виджете **Алерты по статусу** под значком периода отображается количество алертов, сгруппированных по статусам **Новый**, **Открыт**, **Назначен** или **Эскалирован**.
  Если вы хотите просмотреть в легенде алерты только со статусами **Открыт** и **Назначен**, вы можете снять флажки слева от статусов **Новый** и **Эскалирован**.
- На виджете **События**, для которого указан SQL-запрос `SELECT count(ID) AS `metric`, Name AS `value` FROM `events` GROUP BY Name ORDER BY `metric` DESC LIMIT 10`, под значком периода отображается 10 событий, сгруппированных по имени и отсортированных в порядке убывания.
  Если вы хотите просмотреть в легенде события с определенными именами, вы можете снять флажки слева от имен событий, которые не должны отображаться в легенде.

Основные принципы работы с графиками типа Счетчик

На графиках этого типа отображается сумма выбранных данных.

Пример 1
На виджете **Количество активов** отображается общее количество активов, добавленных в KUMA.
Пример 2
Если вы хотите посмотреть тренды для сравнения текущих данных с данными за прошлый период, вы можете создать виджет с отображением восходящих или нисходящих трендов. Тренды настраиваются в следующих виджетах:

- **Активы → Количество активов**.
- **Активы → Пользовательский виджет**.
- **Алерты → Активные алерты**.
- **Алерты → Неназначенные алерты**.
- **Инциденты → Активные инциденты**.
- **Инциденты → Неназначенные инциденты**.
- **Инциденты → Все инциденты**.
- **Пользователи → Количество пользователей AD**.
  Чтобы настроить отображение трендов, необходимо включить переключатель **Показать данные за предыдущий период**, а затем выбрать тренд на вкладке Внешний вид. Если значение в процентах не может быть вычислено или если значения равны, отображается значок `—`. Если выбран параметр **Восходящий - лучше**, зеленая стрелка на графике указывает на восходящий тренд, красная – на нисходящий. Если выбран параметр **Нисходящий - лучше**, красная стрелка на графике указывает на восходящий тренд, зеленая – на нисходящий.
  Если вам нужно изменить отображение данных на виджете (например, вместо процентов посмотреть абсолютные значения), вы можете нажать кнопкой мыши на значение. Эта функция доступна при отображении виджета на панели мониторинга и при включенном режиме ТВ.

Основные принципы работы с графиками типа Таблица

На графиках этого типа данные отображаются в виде таблицы.

Пример:
На виджете **События**, для которого указан SQL-запрос `SELECT TenantID, Timestamp, Name, DeviceProduct, DeviceVendor FROM `events` LIMIT 10`, отображается таблица событий со столбцами **TenantID**, **Timestamp**, **Name**, **DeviceProduct**, **DeviceVendor**. Таблица содержит 10 строк.

Вы можете настроить отображение данных в таблице с помощью градиентной заливки – двухцветной (красно-зеленая) или трехцветной (красно-желто-зеленая). После того как вы выберете тип градиента, вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Для двухцветного градиента задаются два значения, для трехцветного – три. Эти значения отображаются в легенде и определяют, какого цвета маркер будет добавлен в ячейку выбранного столбца. Столбец задается в раскрывающемся списке **Поле с индикатором градиента**.

Основные принципы работы с графиками типа Столбчатая диаграмма

Под списком тенантов отображается столбчатая диаграмма с легендой. В легенде отображаются названия категорий, соответствующих столбцам диаграммы. Из контекстного меню категории в легенде, вы можете перейти в раздел OSMP Console с соответствующими данными. Данные в разделе будут отсортированы в соответствии с фильтрами и/или поисковым запросом, указанным в виджете.

При переходе из легенды виджета в раздел событий для детализации информации обратите внимание на текст элемента легенды, по которому вы переходите в раздел событий. Если в тексте используется символы \ или ', то они будут экранированы в тексте SQL-запроса. При этом символ / не экранируется.

Пример:
На виджете **Netflow top internal IPs**, для которого указан SQL-запрос `SELECT sum(BytesIn) AS metric, DestinationAddress AS value FROM `events` WHERE (DeviceProduct = 'netflow' OR DeviceProduct = 'sflow') AND (inSubnet(DestinationAddress, '10.0.0.0/8') OR inSubnet(DestinationAddress, '172.16.0.0/12') OR inSubnet(DestinationAddress, '192.168.0.0/16')) GROUP BY DestinationAddress ORDER BY metric DESC LIMIT 10`, на оси X диаграммы отображается сумма трафика в байтах, на оси Y диаграммы отображаются адреса портов назначения. Данные сгруппированы по адресам назначения в порядке убывания суммы трафика.

Вы также можете настроить отображение столбцов диаграммы с помощью градиентной заливки – двухцветной (красно-зеленая) или трехцветной (красно-желто-зеленая). После того как вы выберете тип градиента, вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Для двухцветного градиента задаются два значения, для трехцветного – три. Эти значения отображаются в легенде и определяют, как будут окрашены столбцы диаграммы.

Основные принципы работы с графиками типа Календарная диаграмма

Под списком тенантов отображается календарная диаграмма с легендой. В легенде отображаются названия категорий, соответствующих столбцам диаграммы. Из контекстного меню категории в легенде, вы можете перейти в раздел OSMP Console с соответствующими данными. Данные в разделе будут отсортированы в соответствии с фильтрами и/или поисковым запросом, указанным в виджете.

При переходе из легенды виджета в раздел событий для детализации информации обратите внимание на текст элемента легенды, по которому вы переходите в раздел событий. Если в тексте используется символы \ или ', то они будут экранированы в тексте SQL-запроса. При этом символ / не экранируется.

Если при создании виджета с графиком типа **Календарная диаграмма** выбран вид диаграммы **Столбчатая диаграмма**, вы можете настроить отображение столбцов диаграммы с помощью градиентной заливки – двухцветной (красно-зеленая) или трехцветной (красно-желто-зеленая). После того как вы выберете тип градиента, вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Для двухцветного градиента задаются два значения, для трехцветного – три. Эти значения отображаются в легенде и определяют, как будут окрашены столбцы диаграммы.

Пример:

```
SELECT count(ID) AS `metric`, Timestamp AS `value`
FROM `events`
GROUP BY Timestamp
ORDER BY `metric` DESC
LIMIT 250
```

На диаграмме по оси X отсчитывается дата создания события, по оси Y диаграммы отображается количество событий. Столбцы диаграммы расположены слева направо в порядке убывания количества событий.

Если в SQL-запросе используется дополнительное поле с псевдонимом `category`, столбчатая диаграмма отображается в виде сложенной диаграммы. В этом случае градиентная заливка не применяется.

Пример:

```
SELECT count(ID) AS `metric`, Timestamp AS `category`, Type AS `value`
FROM `events`
GROUP BY Timestamp, Type
ORDER BY metric DESC
LIMIT 250
```

На диаграмме по оси X отображаются временные интервалы, по оси Y – количество событий. Каждая часть столбца соответствует значению поля, отмеченного как **Type**.

Если при создании виджета с графиком типа **Календарная диаграмма** выбран вид диаграммы **Линейная диаграмма**, возможны два варианта отображения графика: одна линия (если в запросе указаны только поля `metric` и `value`) и несколько линий (если используется дополнительное поле с псевдонимом `category`). Это позволяет сравнивать между собой значения по различным группам, в зависимости от того, по какому полю выполняется группировка в запросе. Например, это могут быть корреляционные правила, пользователи, устройства. Градиентная заливка к такому графику не применяется.

Пример:

```
SELECT count(ID) AS `metric`, Timestamp AS `category`, CorrelationRuleName AS `value`
FROM `events`
WHERE Type = 3
GROUP BY Timestamp, CorrelationRuleName
ORDER BY metric DESC
LIMIT 250
```

На диаграмме по оси X отображаются временные интервалы (поле, отмеченное как `category`). По оси Y отображается количество срабатываний правил корреляции (поле, отмеченное как `metric`). Каждая линия на графике соответствует уникальному значению поля `value` (в этом случае, названию правила корреляции).

Для группировки вы можете использовать в календарной диаграмме следующие поля времени:

- `Timestamp`
- `DeviceCustomDate1`
- `DeviceCustomDate2`
- `EndTime`
- `FileCreateTime`
- `FileModificationTime`
- `FlexDate1`
- `OldFileCreateTime`
- `OldFileModificationTime`
- `DeviceReceiptTime`
- `StartTime`

> Для полноценной работы с данными, рекомендуется округлять с помощью поддерживаемых функций ClickHouse значения в поле времени (отмеченное как **Timestamp**) до нужного временного интервала (например, 1 час, 1 день).

Для виджета с графиком типа **Календарная диаграмма** с видом диаграммы **Линейная диаграмма** вы также можете настроить параметры для отображения среднего значения. Для этого на вкладке **Внешний вид** для параметра **Регрессия** требуется выбрать **LOESS**.

Основные принципы работы с графиками типа Линейная диаграмма

Под списком тенантов отображается линейная диаграмма с легендой. В легенде отображаются названия категорий, соответствующих линиям на графике. Из контекстного меню категории в легенде, вы можете перейти в раздел OSMP Console с соответствующими данными. Данные в разделе будут отсортированы в соответствии с фильтрами и/или поисковым запросом, указанным в виджете.

При переходе из легенды виджета в раздел событий для детализации информации обратите внимание на текст элемента легенды, по которому вы переходите в раздел событий. Если в тексте используется символы \ или ', то они будут экранированы в тексте SQL-запроса. При этом символ / не экранируется.

Пример:

На виджете **События**, для которого указан SQL-запрос `SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` GROUP BY SourcePort ORDER BY `value` ASC LIMIT 250`, на оси X диаграммы представлен примерный номер порта, на оси Y диаграммы отображаются количество событий. Данные сгруппированы по номеру порта в порядке возрастания.

Для виджета с графиком типа **Линейная диаграмма** вы также можете настроить параметры для отображения среднего значения. Для этого на вкладке **Внешний вид** для параметра **Регрессия** требуется выбрать **Линейная**. Если на графике отображается несколько категорий, для каждой категории отображается среднее значение.

Основные принципы работы с графиками типа Сложенная столбчатая диаграмма

Под списком тенантов отображается сложенная столбчатая диаграмма с легендой. В легенде отображаются названия категорий, составляющих части каждого столбца. Слева от каждой категории находится флажок, с помощью которого можно скрыть или показать категорию. Количество столбцов на диаграмме соответствует количеству значений в выбранной группировке. Столбцы подписаны метками. Цвет соответствующей категории в столбце присваивается автоматически. При наведении курсора мыши на области столбца отображается подсказка со значением и описанием значения. Из контекстного меню категории в легенде можно перейти в раздел OSMP Console с соответствующими данными.

При переходе из легенды виджета в раздел событий для детализации информации обратите внимание на текст элемента легенды, по которому вы переходите в раздел событий. Если в тексте используется символы \ или ', то они будут экранированы в тексте SQL-запроса. При этом символ / не экранируется.

Столбцы имеют разную интерпретацию высоты в зависимости от значения параметра **Формат**:

- Если выбран формат **Абсолютные значения**, то высота столбцов соответствует сумме значений измеряемого показателя.

- Если выбран формат **Относительные значения, %**, то все столбцы имеют одинаковую высоту 100%, а размеры подкрашенных областей столбца соответствуют процентному соотношению между значениями показателя.

Если при создании пользовательского виджета на основе сложенной столбчатой диаграммы выбран параметр **Показывать данные за предыдущий период** и в запросе указаны стандартные псевдонимы `value`, `category`, `metric`, то на диаграмме отдельными столбцами показываются данные предыдущего периода. Если же в запросе вместо стандартной метрики `metric` применяется пользовательский расчет метрик с нестандартными псевдонимами, то параметр **Показывать данные за предыдущий период** не будет учитываться при построении диаграммы (см. примеры запросов ниже).

Примеры:
При создании пользовательского виджета с графиком типа **Сложенная столбчатая диаграмма** на основе SQL-запроса для виджета **События** действуют следующие правила:

- Поле в запросе, отмеченное как псевдоним `value` (должно быть указано обязательно), будет использоваться на диаграмме как поле, по которому строится легенда и столбцы делятся на категории.
- Поле в запросе, отмеченное как псевдоним `category` (должно быть указано обязательно), будет использоваться на диаграмме как поле, по значениям которого будут расположены столбцы по оси X.
- Поле в запросе, отмеченное как псевдоним `metric`, будет использоваться на диаграмме как поле, по которому должен вестись количественный подсчет частей столбцов. В этом случае количественное распределение будет производиться автоматически.

При этом вы можете самостоятельно управлять подсчетом, используя в качестве метрик стандартные функции агрегации `sum`, `avg`, `min`, `max`, `count` и собственные псевдонимы с произвольным названием вместо стандартного псевдонима `metric` (в этом случае не будет поддерживаться отображение данных за предыдущий период).

Пример 1:
В виджете **События** указан следующий SQL-запрос со стандартными псевдонимами, при создании виджета выбран параметр **Показывать данные за предыдущий период**:

```
SELECT count(ID) AS `metric`,

Type AS `value`,

TenantID AS `category`

FROM `events`

GROUP BY value, category

ORDER BY metric DESC
```

На диаграмме по оси X отображаются соответствующие тенанты (поле, отмеченное как `category`), по оси Y отображается количество событий определенного типа (поле, отмеченное как value). В каждом столбце количество, соответствующее определенному типу, отображается отдельным цветом. В легенде в качестве категорий отображаются названия типов событий, по которым разбиваются столбцы. Каждой категории соответствует цвет, автоматически присвоенный ей на столбце. Если вы хотите просмотреть на диаграмме события только с определенными типами, вы можете снять или установить флажки слева от соответствующих типов событий в легенде.

Рядом с каждым столбцом отображается дополнительный столбец с данными за прошлый период, если такие данные получены в запросе.

Пример 2:
В виджете **События** указан следующий SQL-запрос с пользовательскими метриками, отмеченными как псевдонимы `Base` и `Audit` вместо стандартного `metric`:

```
SELECT SUM(IF (Type = 1,1,0)) AS `Base`,

SUM(IF (Type = 4,1,0)) AS `Audit`,

TenantID as `category`

FROM `events`

GROUP BY category
```

На диаграмме по оси X отображаются соответствующие тенанты (поле, отмеченное как `category`), по оси Y отображается количество событий каждого типа (пользовательские метрики, отмеченные как псевдонимы Base и Audit). В каждом столбце количество, соответствующее определенной метрике, отображается отдельным цветом. В легенде в качестве названий категорий отображаются метрики `Base` и `Audit`, по которым столбцы делятся на категории. Каждой категории соответствует цвет, автоматически присвоенный ей на столбце. Если вы хотите просмотреть на диаграмме события, соответствующие только определенной метрике, вы можете снять или установить флажки слева от нужной метрики в легенде.

Дополнительный столбец с данными за прошлый период для запроса с пользовательскими метриками не отображается, даже если при создании виджета выбран параметр Показывать данные за предыдущий период.

Пример 3:
В виджете **События** указан следующий SQL-запрос со стандартными псевдонимами:

```
SELECT count(ID) AS `metric`,

TenantID as `value`,

Type as `category`
```

```
FROM events

GROUP BY value, category

ORDER BY metric DESC
```

В отличие от схожего запроса в примере 1, в этом случае на диаграмме по оси X отображаются соответствующие типы событий (поле, отмеченное как `category`), а тенантам (поле, отмеченное как `value`) соответствуют области значений в столбцах (по оси X) и соответствующие подписи в легенде.

Пример 4:
В виджете **События** указан следующий SQL-запрос со стандартными псевдонимами:

```
SELECT count(ID) AS `metric`,

CAST(fromUnixTimestamp64Milli(Timestamp) AS DATE) AS `category`,

Type as `value`

FROM `events`

GROUP BY category, value

ORDER BY category DESC
```

На диаграмме по оси X отображаются дни месяца (поле, отмеченное как `category`). По оси Y отображается количество событий определенного типа (поле, отмеченное как `value`).

Чтобы построить подобный график с расположением столбцов по дате и/или времени, используйте в запросе группировку и сортировку по следующим полям с типом `timestamp`:

- `Timestamp`
- `DeviceCustomDate1`
- `DeviceCustomDate2`
- `EndTime`
- `FileCreateTime`
- `FileModificationTime`
- `FlexDate1`
- `OldFileCreateTime`
- `OldFileModificationTime`
- `DeviceReceiptTime`
- `StartTime`

> Для полноценной работы с данными, расположенными по дате и/или времени, рекомендуется использовать тип графиков **Календарная диаграмма**.

Основные принципы работы с графиками типа Спидометр

На графиках этого типа отображается процентное отношение количества объектов выбранной категории к общему количеству объектов за определенный период. **Спидометр** строится для следующих объектов:

- для активов в выбранной категории, удовлетворяющих заданному условию, относительно общего количества активов в этой категории или некатегоризированных активов;
- для удовлетворяющих заданному условию алертов относительно общего количества алертов за определенный период;
- для удовлетворяющих заданному условию инцидентов относительно общего количества инцидентов;
- для удовлетворяющих заданному условию событий относительно общего количества событий за определенный период.

Значение на графике отображается в процентах с цветовой градацией по настроенным интервалам значений. По умолчанию указаны следующие интервалы процентных значений: 0–30, 30–70, 70–100.

Пример 1:
На пользовательском виджете **Активы** пользователь выбирает категорию активов, количество активов в которой сравнивается с общим количеством активов. Пользователь может указать пороговые значения для шкалы на графике. Затем на основе одного или нескольких условий для оси Y осуществляется расчет по имеющейся базе активов.

Пример 2:
На виджете **Алерты** тип **Спидометр** можно выбрать для категорий **Активные алерты** и **Неназначенные алерты**. Для алертов выбираются тенант и период для анализа. По умолчанию эти значения соответствуют значениям, указанным в применимой панели мониторинга. В общем количестве алертов можно также показать данные за предыдущий период.

Аналогичным образом рассчитывается процентное значение для категорий **Активные инциденты** и **Неназначенные инциденты** на виджете **Инциденты**.

Пример 3:
На виджете **События** для типа **Спидометр** пользователь указывает тенанта, период для анализа, а также хранилище данных о событиях. SQL-запрос к базе данных отображается в следующем виде:

```
SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` GROUP BY SourcePort ORDER BY value ASC LIMIT 250
```

Особенности отображения данных в виджетах

Ограничение отображаемых данных

Для удобства восприятия информации в Kaspersky SIEM Cloud заданы ограничения на отображение данных в виджетах в зависимости от их типа:

- Круговая диаграмма – отображается не более 20 отсеков.
- Столбчатая диаграмма – отображается не более 40 столбцов.
- Таблица – отображается не более 500 записей.
- Календарная диаграмма – отображается не более 365 дней.

Данные, выходящие за указанные ограничения, отображаются в виджете в категории **Остальное**.

Все данные, по которым построена аналитика в виджете, можно скачать в формате CSV.

Суммирование данных

Формат отображения итоговой суммы данных на календарной, столбчатой и круговой диаграммах зависит от языка локализации:

- Английская локализация: порядки разделяются запятыми, дробная часть отделяется точкой.
- Русская локализация: порядки разделяются пробелами, дробная часть отделяется запятой.

Создание виджета

Вы можете создать виджет в макете панели мониторинга во время создания или изменения макета.

Чтобы создать виджет:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Создайте макет или переключитесь в режим редактирования для выбранного макета.
3. Нажмите на кнопку **Добавить виджет**.
4. В раскрывшемся списке выберите тип виджета.

   Откроется окно с параметрами виджета.
5. Измените параметры виджета.
6. Если вы хотите увидеть, как данные будут отображаться в виджете, нажмите на кнопку **Предварительный просмотр**.
7. Нажмите на кнопку **Добавить**.

Виджет появится на макете в панели мониторинга.

Изменение виджета

Чтобы изменить виджет:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Раскройте список в правом верхнем углу окна.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на кнопку **Изменить** ( ).
5. В виджете, который вы хотите изменить, нажмите на значок меню ( ).
6. Выберите **Изменить**.

   Откроется окно с параметрами виджета.
7. Измените параметры виджета.

8. Нажмите на кнопку **Сохранить** в окне свойств виджета.

9. Нажмите на кнопку **Сохранить** в окне **Настройка макета**.

Виджет изменен.

Удаление виджета

Чтобы удалить виджет:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.

2. Раскройте список в правом верхнем углу окна.

3. Наведите курсор мыши на соответствующий макет.

4. Нажмите на кнопку **Изменить** ( ).

5. В виджете, который вы хотите удалить, нажмите на значок параметров ( ).

6. Выберите пункт **Удалить**.

7. В открывшемся окне подтверждения нажмите на кнопку **OK**.

8. Нажмите на кнопку **Сохранить**.

Виджет удален.

Параметры виджетов

Этот раздел содержит описание параметров всех доступных в Kaspersky SIEM Cloud виджетов.
Виджет События
Вы можете использовать виджет **События** для получения необходимой аналитики на основе SQL-запросов.

При создании этого виджета вам требуется указать значения для параметров, описанных в таблицах ниже.

Вкладка Общие

В таблице ниже описаны параметры, расположенные на вкладке **Общие**.

Описание параметров

Параметр	Описание
Название	Название виджета. При сохранении отчета в формате Excel название виджета, отображаемое в заголовке листа, ограничено 31 символом. Рекомендуется называть виджеты с учетом этого ограничения.
График	Тип графика. Доступны следующие типы графиков: • **Круговая диаграмма**. • **Столбчатая диаграмма**. • **Счетчик**. • **Линейная диаграмма**. • **Таблица**. • **Календарная диаграмма**. • **Столбчатая диаграмма с накоплением**. • **Спидометр**.

Параметр	Описание
Формат	Формат отображения данных: **Абсолютные значения** или **Относительные значения, %**. Параметр доступен для графика типа **Столбчатая диаграмма с накоплением**. При выборе формата **Абсолютные значения** высота столбцов диаграммы соответствует сумме значений измеряемого показателя. При выборе формата **Относительные значения, %** все столбцы имеют одинаковую высоту 100%, а размеры цветных областей столбца соответствуют процентному соотношению между значениями показателя. По умолчанию выбрано **Абсолютные значения**.
Вид временной диаграммы	Формат отображения временных данных: **Столбчатая диаграмма** или **Линейная диаграмма**. Параметр доступен для графика типа **Календарная диаграмма**. При выборе формата **Столбчатая диаграмма** данные по умолчанию отображаются в виде вертикальных столбцов. Если SQL-запрос содержит дополнительное поле с псевдонимом `category`, столбчатая диаграмма будет представлена в виде сложенной диаграммы, то есть с разбивкой каждого столбца по значениям этого поля. При выборе формата **Линейная диаграмма** данные отображаются в виде одной или нескольких (в зависимости от запроса) ломаных линий, соединяющих точки на временной оси. По умолчанию выбран формат **Столбчатая диаграмма**.
Период	Период, за который отображаются данные на виджете. По умолчанию выбрано **Как на макете** – отображаются данные за период, выбранный для макета. Вы также можете указать период для виджета одним из следующих способов: • Выбрать точные дату и время начала и окончания периода в календаре и нажать на кнопку **Применить**. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: выбрать точные дату и время или относительный период либо использовать комбинацию этих способов. Подробнее см. ниже в подразделе *Настройка значения периода*.
Показывать данные за предыдущий период	Включение отображения данных сразу за два периода: за текущий и за предыдущий. При использовании графика типа **Столбчатая диаграмма с накоплением** параметр **Показывать данные за предыдущий период** будет учитываться, если в запросе указаны стандартные псевдонимы `value`, `category`, `metric`. Если же в запросе вместо стандартной метрики `metric` используется пользовательский расчет метрик с нестандартными псевдонимами, то параметр **Показывать данные за предыдущий период** учитываться не будет.
Доступные переменные	Локальные или глобальные переменные, которые вы можете использовать для фильтрации данных виджета. Нажмите на кнопку **Добавить**. Если вы добавляете локальную переменную, введите произвольное имя переменной, затем укажите значение переменной. Если вы добавляете глобальную переменную, выберите из списка имя переменной, которую вы указали в свойствах панели мониторинга.
Хранилище	Хранилище, в котором выполняется поиск событий. В списке отображаются доступные пространства. Можно выбрать только одно хранилище, можно выбрать одно или несколько пространств. В поле отображаются хранилища и пространства, как в разделе **События**. Если в хранилище было создано новое пространство, в параметрах виджета новое пространство по умолчанию не выбрано. Следует выбрать новое пространство вручную. Если у пользователя есть доступ ко всем пространствам, указанным в виджете, тогда на виджете будут доступны для просмотра данные по событиям, указанным в наборе пространств и в правах пользователя. Если у пользователя нет прав доступа к одному или нескольким пространствам хранилища, данные на виджете будут недоступны для просмотра, пользователь не может редактировать виджет, но может продублировать виджет с помощью кнопки **Дублировать**. Дублирование не зависит от прав доступа к пространствам. При дублировании шаблона в тех виджетах, где были указаны недоступные пользователю пространства, значение в поле **Хранилище** будет сброшено. В таких виджетах будет отображаться ошибка Access denied (Operation returns no results because of allowed and selected event spaces). Для сохранения шаблона необходимо указать пространства в виджетах. В тех виджетах, где были указаны пространства, доступные пользователю, значение поля **Хранилище** не сбрасывается и сохраняется при дублировании шаблона. При выгрузке отчета пользователь получит файл, в котором скрыты данные недоступных виджетов. Если адрес электронной почты пользователя указан в списке получателей отчета по расписанию, пользователь получит полную версию отчета независимо от доступных пространств.

Параметр	Описание

Поле SQL-запроса	Запрос для фильтрации и поиска событий вручную. Вы можете составить запрос в конструкторе запросов, нажав на кнопку **Использовать конструктор SQL**.
	Вы можете использовать поля расширенной схемы событий для построения графика типа **Таблица**.
	Пример
	Предварительное условие:
	Из FWSaaS-системы поступают события.
	10.08.2023 12:12:12 src=10.10.10.10 ReqUrls=[https://google.com, https:/ya.ru]
	10.08.2023 12:12:23 src=10.10.10.20 ReqUrls=[https://google.com, https:/yandex.ru]
	10.08.2023 12:12:33 src=10.10.10.30 ReqUrls=[https://google.com, https:/ya.ru, https://mail.ru]
	Главный администратор Kaspersky SIEM Cloud добавил поле расширенной схемы событий в разделе Kaspersky SIEM Cloud **Параметры → Другое → Поля расширенной схемы событий**. В нормализаторе Kaspersky SIEM Cloud настроено сопоставление полей **ReqUrls** и **SA.urls**.
	В Kaspersky SIEM Cloud нормализованные события выглядят следующим образом:
	DeviceReceiptTime=10.08.2023 12:12:12 SourceAddress=10.10.10.10 SA.urls=[https://google.com, https:/ya.ru]
	DeviceReceiptTime=10.08.2023 12:12:23 SourceAddress=10.10.10.20 SA.urls=[https://google.com, https:/yandex.ru]
	DeviceReceiptTime=10.08.2023 12:12:30 SourceAddress=10.10.10.30 SA.urls=[https://google.com, https:/ya.ru, https://mail.ru]
	Вы хотите построить панель мониторинга Top URLs за 30 мин. Пример запроса в разделе **События** и в виджетах:
	SELECT res.1 AS url, res.2 AS count FROM (SELECT arrayJoin(groupArray((url, count))) AS res FROM (SELECT url, count() AS count FROM (SELECT SA.urls AS urls FROM `events`) ARRAY JOIN urls AS url GROUP BY url) GROUP BY url)
	Результат:
	url count
	google.com 3
	ya.ru 2
	mail.ru 1
	yandex.ru 1
	В Kaspersky SIEM Cloud поддержаны следующие функции, которые позволяют использовать в запросах массивы:
	• `groupArray` — собирает все значения аргумента x в массив и используется в агрегатных функциях при группировке данных.
	• `arrayJoin` — раскрывает массив на отдельные строки в результате выполнения запроса.
	При составлении SQL-запроса вы можете использовать переменные. Переменные можно указывать только при составлении запроса вручную. В конструкторе SQL переменные использовать нельзя.
	Пример с использованием переменных
	`Пример SQL-запроса с использованием локальной переменной`
	`SELECT count(ID) AS 'metric', Name AS 'value', TenantID AS 'category' FROM 'events' WHERE filter(Name = $Name) GROUP BY Name, TenantID ORDER BY metric DESC LIMIT 250`
	В этом запросе использована локальная переменная `$Name`. В эту переменную будет подставляться значение из поля события `Name`. Вы можете применить переменную, нажав на значок воронки ( ) на виджете. В открывшемся окне вы сможете выбрать значение для переменной. Виджет отфильтрует выборку по выбранному значению поля `Name`.
	Обратите внимание, если в SQL-запросе вы указываете переменную для поля, которое принимает числовое значение, такое значение надо преобразовать в строку. Для этого используйте функцию `toString`. Иначе SQL-запрос вернет ошибку.
	`Пример`
	`SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` WHERE (filter(toString(SourcePort) like $SourcePort)) GROUP BY SourcePort ORDER BY value ASC LIMIT 250`
	В этом запросе поле события `SourcePort` имеет числовое значение, поэтому оно преобразовано в строку `toString(SourcePort)`.
	Подробнее о создании SQL-запроса в конструкторе запроса см. ниже.
	Существуют следующие ограничения:
	• Псевдонимы `metric` и `value` в SQL-запросах недоступны для изменения для всех типов виджета с аналитикой по событиям, кроме таблиц.
	• Псевдонимы в виджетах с графиком типа **Таблица** могут содержать латинские и кириллические символы, а также пробелы. При использовании пробелов или кириллицы псевдоним необходимо выделять кавычками: `"Псевдоним с пробелом"`, `` `Другой псевдоним` ``.

Параметр	Описание
	• Не поддерживается использование SQL-запроса `ARRAY JOIN`. • При отображении данных за предыдущий период сортировка по параметру `count(ID)` может работать неправильно. Мы рекомендуем использовать сортировку по параметру `metric`. Например, `SELECT count(ID) AS "metric", Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250`. • В виджетах с графиком типа **Счетчик** для значений функции `SELECT` требуется указывать способ обработки данных: `count`, `max`, `min`, `avg`, `sum`. • В виджетах с графиком типа **Таблица** градиент строится по значениям числового или временного поля (например, `Timestamp`), указанного в SQL-запросе. Это поле можно выбрать в раскрывающемся списке **Поле с индикатором градиента** (если в запросе указано несколько числовых или временных полей, они все будут доступны для выбора). После этого ячейки выбранного столбца будут подсвечены маркерами градиентной заливки. Если поле отсутствует в запросе, на вкладке **Внешний вид** не отображаются поля **Градиент** и **Поле с индикатором градиента**. • В виджетах с графиком типа **Столбчатая диаграмма с накоплением** значения временного поля `Timestamp` не отображаются по оси X при использовании стандартного запроса. Если требуется отображать время по оси X, рекомендуется использовать график типа **Линейная диаграмма**. Если вам нужно использовать график типа **Столбчатая диаграмма с накоплением**, значение `Timestamp` необходимо конвертировать в строку `toString(Timestamp) AS `category``.

Настройка значения периода

Чтобы настроить период отображения данных, выполните одно из следующих действий:

- При необходимости измените дату и время в параметре **Период** одним из следующих способов:

  - Если вы хотите указать **точную дату**, в календаре выберите даты начала и окончания периода и нажмите на кнопку **Применить**.

    Вы можете выбрать дату до текущей включительно. Формат даты и времени зависит от параметров вашего браузера. Если в поле **Дата от** или **Дата до** есть значение и вы не меняли вручную значение времени, при выборе даты в календаре в поле **Дата от** автоматически подставится время `00:00:00.000`, а в поле **Дата до** – `23:59:59.999`. Если вы вручную удалили значение в поле **Дата от** или **Дата до**, при выборе даты в календаре в поле автоматически подставится текущее время. После того как вы выберете значение в одном из полей, фокус переключается на другое поле. Если в поле **Дата до** вы выбираете значение, которое меньше значения в поле **Дата от**, это меньшее значение будет автоматически подставлено в поле **Дата от**.

  - Если вы хотите указать **относительный период**, выберите один из доступных периодов в списке **Относительный период**.

    Период рассчитывается относительно настоящего времени.

  - Если вы хотите указать **пользовательский период**, задайте или измените значение вручную в полях **Дата от** и **Дата до**.

    Вы можете указать точные дату и время в формате `DD.MM.YYYY HH:mm:ss.SSS` для русской локализации и `YYYY-MM-DD HH:mm:ss.SSS` для английской локализации или период относительно текущего времени в виде формулы. Вы также можете комбинировать эти способы. Если при вводе точной даты вы не указали миллисекунды, автоматически подставляется значение `000`. Если вы вручную изменили время в полях **Дата от** или **Дата до**, при переключении даты в календаре значение времени не меняется.

    В формулах относительного периода используйте параметр `now` для обозначения текущих даты и времени и язык параметризации интервалов: символы `+` (только в поле **Дата до**), `-`, `/` (округление до ближайшего), а также единицы изменения времени `y` (год), `M` (месяц), `w` (неделя), `d` (день), `h` (час), `m` (минута), `s` (секунда). Например, вы можете указать период `now-5d`, чтобы получить данные за последние пять дней, или `now/w`, чтобы получить данные с начала первого дня текущей недели (00:00:00:000 в UTC) до текущего времени `now`.

Поле **Дата от** является обязательным, и его значение не может превышать значение, установленное в поле **Дата до**, а также не может быть меньше 01.01.1970 (при указании точной даты или относительного периода). Значение в поле **Дата до** не должно быть меньше значения, установленного в поле **Дата от**. Если вы не укажете значение в поле **Дата до**, параметр `now` указывается автоматически.

Время в Kaspersky SIEM хранится в UTC, но в веб-интерфейсе оно конвертируется в соответствии с часовым поясом вашего браузера. Это нужно учитывать для относительных периодов **Сегодня**, **Вчера**, **Эта неделя** и **Этот месяц**. Например, если в браузере установлен часовой пояс UTC+3 и вы выбрали период отображения данных **Сегодня**, данные будут отображаться за период с 03:00:00.000 до текущего времени, а не с 00:00:00.000.

Если при выборе относительного периода **Сегодня**, **Вчера**, **Эта неделя** или **Этот месяц** вы хотите отобразить данные в соответствии с вашим часовым поясом, вам нужно вручную добавить сдвиг по времени в поля **Дата от** и **Дата до** (если указано значение кроме `now`), прибавив или убавив необходимое количество часов. Например, если в браузере установлен часовой пояс UTC+3 и вы хотите отобразить данные за период **Вчера**, вам нужно изменить значение в поле **Дата от** на `now-1d/d-3h`, а в поле **Дата до** – на `now/d-3h`. Если же вы хотите отобразить данные за период **Сегодня**, вам нужно изменить значение только в поле **Дата от** на `now/d-3h`.

Если вам нужны результаты до 23:59:59:999 вчерашнего дня в UTC, то используйте SQL-запрос с фильтром по Timestamp или укажите точные дату и время.

Границы периода включаются: например, для периода **Сегодня** отобразятся события с начала сегодняшнего дня 00:00:00:000 в UTC до текущего времени **now** включительно, а для периода **Вчера** – с начала вчерашнего дня 00:00:00:000 до 00:00:00:000 в UTC сегодняшнего дня. Вы можете посмотреть дату и время последнего обновления данных и точный период, за который отображаются данные, наведя курсор на значок периода на виджете.

Если для виджета вы включили параметр **Показывать данные за предыдущий период**, и данные на виджете отображаются за относительный период, во всплывающей подсказке также будет отображаться предыдущий период. Предыдущий период рассчитывается относительно текущего периода как значения начала и конца текущего периода минус длительность текущего периода. Например, если данные обновляются ежедневно и отображаются за месяц, но прошли только первые 10 дней месяца, прошлым периодом будут считаться последние 10 дней прошлого месяца.

- Если вы хотите отобразить на виджете данные за период, выбранный для макета, вы можете нажать на кнопку **Сбросить**. При изменении периода отображения данных на макете, также изменится отображаемый на виджете период.

Как создать запрос в конструкторе запросов

Чтобы создать запрос в конструкторе запросов:

1. Укажите значения для следующих параметров:

   a. **SELECT** – поля событий, которые следует возвращать. Количество доступных полей зависит от выбранного типа графика.

   - В раскрывающемся списке слева выберите поля событий, данные по которым должны отображаться на виджете.
   - Среднее поле показывает, для чего выбранное поле используется в виджете: **metric** (метрики) или **value** (значение).

     Если вы выбрали тип графика **Таблица**, в средних полях нужно указать названия столбцов, используя символы ANSII-ASCII.

   - В раскрывающемся списке справа вы можете выбрать операцию, которую следует произвести над данными:
     - **count** – подсчет событий. Эта операция доступна только для поля события **ID**. Используется по умолчанию для линейных, круговых и столбчатых диаграмм, а также для счетчиков. Является единственно возможным вариантом для календарных диаграмм.
     - **max** – максимальное значение поля **события** из выборки событий.
     - **min** – минимальное значение поля **события** из выборки событий.
     - **avg** – среднее значение поля **события** из выборки событий.
     - **sum** – сумма значений полей событий из выборки событий.

   b. **SOURCE** – тип источника данных. Для выбора доступно только значение **events** (события).

   c. **WHERE** – условия фильтрации событий.

   - В раскрывающемся списке слева выберите поле события, которое вы хотите использовать для фильтрации.
   - В среднем раскрывающемся списке выберите нужный оператор. Доступные операторы зависят от типа значения выбранного поля события.
   - В раскрывающемся списке справа введите значение условия. В зависимости от выбранного типа поля вам потребуется ввести значение вручную, выбрать его в раскрывающемся списке или выбрать в календаре.

   Вы можете добавить условия поиска, нажав на кнопку **Добавить условие** или удалить их, нажав на кнопку ✕.

   Вы можете добавить группы условий, нажав на кнопку **Добавить группу**. По умолчанию группы условий добавляются с оператором **AND**, но при необходимости вы можете изменить значение. Доступные значения: **AND**, **OR**, **NOT**. Группы условий удаляются с помощью кнопки **Удалить группу**.

   d. **GROUP BY** – поля событий или псевдонимы, по которым следует группировать возвращаемые данные. Этот параметр недоступен для графиков типа **Счетчик**.

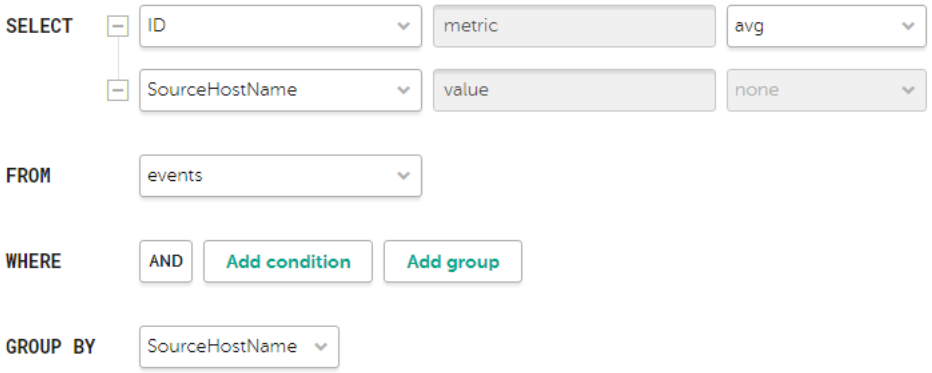
e. **ORDER BY** – столбцы, по которым следует сортировать возвращаемые данные. Этот параметр недоступен для графиков следующих типов: **Календарная диаграмма** и **Счетчик**.

- В раскрывающемся списке слева выберите значение, которое будет использоваться для сортировки.
- В раскрывающемся списке справа выберите порядок сортировки: **ASC** – по возрастанию, **DESC** – по убыванию.
- Для графиков типа **Таблица** можно добавить условия сортировки с помощью кнопки **Добавить столбец**.

f. **LIMIT** – максимальное количество точек данных для виджета. Этот параметр недоступен для графиков типа **Календарная диаграмма** и **Счетчик**.

2. Нажмите на кнопку **Применить**.

Пример условий поиска в конструкторе запросов



Параметры условий поиска для отображения в виджете среднего количества байт в расчете на один хост

Вкладка Оси

В таблице ниже описаны параметры, расположенные на вкладке **Оси**.

Вкладка отображается, если на вкладке **Общие** в поле **График** вы выбрали одно из следующих значений: **Столбчатая диаграмма**, **Линейная диаграмма**, **Календарная диаграмма**.

Описание параметров

Параметр	Описание
Размер указателя	Размер указателя на графике. Поле отображается для типа графика **Линейная диаграмма**.
Толщина линии	Толщина линии на графике. Поле отображается для типа графика **Линейная диаграмма**.
Минимальное и максимальное значение для оси Y	Масштаб оси Y. На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.

Параметр	Описание
Минимальное и максимальное значение для оси X	Масштаб оси X. На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.
Десятичные знаки	Количество десятичных знаков, до которых отображаемое значение должно быть округлено.

Вкладка Внешний вид

В таблице ниже описаны параметры, расположенные на вкладке **Внешний вид**.

Описание параметров

Параметр	Описание
Описание	Описание виджета.
Легенда	Отображение легенды для аналитики. По умолчанию переключатель включен.
Пустые значения в легенде	Отображение параметров с нулевым значением в легенде для аналитики. По умолчанию переключатель включен. Пустые значения отображаются только при включенном параметре **Показать данные за предыдущий период**, если в текущем периоде данных нет, а в предыдущем были.
Цвет	Цвет отображения информации: • **по умолчанию** – цвет шрифта, который используется в вашем браузере по умолчанию; • **зеленый**; • **красный**; • **синий**; • **желтый**. Параметр доступен для графиков типа **Столбчатая диаграмма**, **Счетчик**, **Линейная диаграмма**, **Календарная диаграмма**.
Градиент	Градиентная заливка графика: • двухцветная (красно-зеленая); • трехцветная (красно-желто-зеленая). Параметр доступен для графиков типа **Столбчатая диаграмма**, **Календарная диаграмма** (с видом диаграммы **Столбчатая диаграмма**), **Таблица**. Вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Если границы градиента не заданы вручную, они рассчитываются автоматически по значениям данных. Если между заданными границами нет данных, градиент не применяется. Вместо него используется два цвета: один для значений ниже нижней границы, другой – для значений выше верхней.
Поле с индикатором градиента	Столбец, в котором отображаются маркеры градиентной заливки. Параметр доступен для графика типа **Таблица**.
Горизонтальный	Использование горизонтальной гистограммы вместо вертикальной. При включении этого параметра горизонтальная прокрутка при большом количестве данных не будет отображаться и вся имеющаяся информация будет отражена в заданном размере виджета. Если данных для отображения много, рекомендуется увеличить размер виджета.
Итоговые значения	Отображение суммы значений. Округление значения зависит от значения параметра **Десятичные знаки**. Параметр доступен для графиков типа **Круговая диаграмма**, **Столбчатая диаграмма** и **Календарная диаграмма**. По умолчанию переключатель выключен.
Длительность отрезков периода	Длительность отрезков, на которые требуется делить период. Доступно для графика типа **Календарная диаграмма**.
Шкала	Шкала для отображения данных. Доступно для графика типа **Столбчатая диаграмма с накоплением**. Возможны следующие значения: • **Линейная**. • **Квадратичная**. • **Логарифмическая**. По умолчанию выбрано значение **Линейная**.

Параметр	Описание
Регрессия	Вариант указания среднего значения на графике. Возможны следующие значения: • **Не выбрано**. • **Линейная**. • **LOESS** (кривая с локально взвешенным сглаживанием диаграмм рассеяния). Доступно для графиков типа **Календарная диаграмма** и **Линейная диаграмма**.

Вкладка Действия

Вкладка не отображается, если на вкладке **Общие** в поле **График** вы выбрали одно из следующих значений: **Счетчик**, **Спидометр**, **Таблица**.

На вкладке представлены параметры для настройки действий по щелчку левой кнопкой мыши на различных элементах виджетов, например, на сегменте графика или тексте элемента легенды. Вы можете выбрать следующие действия:

- Переход в события.
- Фильтрация по переменной.

  Параметры описаны в сценарии фильтрации данных на нескольких виджетах.
- Переход в другую панель мониторинга.

  Параметры описаны в сценарии перехода в другую панель мониторинга.

Виджет Активные листы

Вы можете использовать виджет **Активные листы** для получения аналитики на основе SQL-запросов.

При создании этого виджета вам требуется указать значения для параметров, описанных в таблицах ниже.

Вкладка Общие

В таблице ниже описаны параметры, значение которых требуется указать на вкладке **Общие**.

Описание параметров

Параметр	Описание
График	Тип графика. Доступны следующие типы графиков: • **Столбчатая диаграмма** • **Круговая диаграмма** • **Счетчик** • **Таблица**
Коррелятор	Название коррелятора, содержащего активный лист, по которому вы хотите получать данные.
Активный лист	Название активного листа, по которому вы хотите получать данные. Один и тот же активный лист может использоваться в разных корреляторах. При этом для каждого коррелятора создается своя сущность активного листа. Таким образом, содержимое активных листов, используемых разными корреляторами, различается, даже если идентификатор и название активных листов одинаковые.

Параметр	Описание
Поле SQL-запроса	В этом поле вы можете ввести запрос для фильтрации и поиска данных активного листа вручную. Структура запроса аналогична той, которая используется при поиске событий. При создании запроса по активным листам вам нужно учитывать следующие особенности: • Для функции FROM требуется указать значение `records`. • Если вы хотите получать данные по полям, названия которых содержат пробелы и символы кириллицы, в запросе такие названия требуется выделять кавычками: • в функции SELECT псевдонимы следует выделять двойными или косыми кавычками: "псевдоним", `другой псевдоним`; • в функции ORDER BY псевдонимы следует выделять косыми кавычками: `другой псевдоним`; • Значения полей событий выделяются прямыми кавычками: WHERE DeviceProduct = 'Microsoft'. • Название полей событий выделять кавычками не требуется. • Если название поля активного листа начинается или заканчивается пробелами, в виджете эти пробелы не отображаются. Название поля не должно состоять только из пробелов. • Если значения полей активного листа могут содержать пробелы в конце или в начале, поиск по ним рекомендуется осуществлять с помощью функции LIKE '%значение поля%'. • Вы можете использовать в запросе служебные поля _key (поле с ключами записей активного листа) и _count (сколько раз эта запись была добавлена в активный лист), а также пользовательские поля. • Псевдонимы metric и value в SQL-запросах недоступны для изменения для всех типов виджета с аналитикой по активным листам, кроме таблиц. • Если в SQL-запросе используется функция преобразования даты и времени (например, fromUnixTimestamp64Milli) и при этом обрабатываемое поле не содержит даты и времени, в виджете будет отображаться ошибка. Чтобы избежать этого, используйте функции, которые могут обрабатывать нулевое значение. Например: SELECT _key, fromUnixTimestamp64Milli(toInt64OrNull(DateTime)) as Date FROM `records` LIMIT 250. • Если задать большие значения для функции LIMIT, это может привести к ошибкам в работе браузера. • Если в качестве типа графика вы выбрали Счетчик, необходимо для значений функции SELECT указывать способ обработки данных: `count`, `max`, `min`, `avg`, `sum`. • В виджетах с графиком типа **Таблица** градиент строится по значениям поля, указанного в SQL-запросе (например, `_count`, `value`, `temp` или `name`). Это поле можно выбрать в раскрывающемся списке **Поле с индикатором градиента** (если в запросе указано несколько числовых или временных полей, они все будут доступны для выбора). После этого ячейки выбранного столбца будут подсвечены маркерами градиентной заливки. Если поле отсутствует в запросе, на вкладке **Внешний вид** не отображаются поля **Градиент** и **Поле с индикатором градиента**. Особенности использования псевдонимов в SQL-функциях: и SELECT допустимо использовать двойные и косые кавычки: ", `. Если в качестве типа графика вы выбрали Счетчик, псевдонимы могут содержать латинские и кириллические символы, а также пробелы. При использовании пробелов или кириллицы псевдоним необходимо выделять кавычками: "Псевдоним с пробелом", `Другой псевдоним`. При отображении данных за предыдущий период сортировка по параметру count(ID) может работать некорректно. Рекомендуется использовать сортировку по параметру metric. Например, SELECT count(ID) AS "metric", Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250.

Примеры запросов для получения аналитики по активным листам:

- `SELECT * FROM `records` WHERE "Источник событий" = 'Екатеринбург' LIMIT 250`
  Запрос, который возвращает ключ активного листа с названием поля "Источник событий" и значением этого поля "Екатеринбург".
- `SELECT count(_key) AS metric, Status AS value FROM `records` GROUP BY value ORDER BY metric DESC LIMIT 250`
  Запрос для круговой диаграммы, который возвращает количество ключей активного листа (агрегация count по полю _key) и все варианты значений пользовательского поля Status. В виджете отображается круговая диаграмма с общим количеством записей активного листа, пропорционально разделенным на количество вариантов значений поля **Status**.
- `SELECT Name, Status, _count AS Number FROM `records` WHERE Description ILIKE '%ftp%' ORDER BY Name DESC LIMIT 250`
  Запрос для таблицы, которая возвращает значения пользовательских полей **Name** и **Status**, а также служебного поля "_count" у тех записей активного листа, в которых значения пользовательского поля Description соответствует запросу ILIKE '%ftp%'. В виджете отображается таблица со столбцами **Status**, **Name** и **Number**.

Вкладка Оси

В таблице ниже описаны параметры, значение которых требуется указать на вкладке **Оси**.

Вкладка отображается, если на вкладке **Общие** в поле **График** вы выбрали значение **Столбчатая диаграмма**.

Описание параметров

Settings	Описание
Минимальное значение Y и Максимальное значение Y	Масштаб оси Y. На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.
Минимальное значение X и Максимальное значение X	Масштаб оси X. На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.

Вкладка Внешний вид

В таблице ниже описаны параметры, значение которых требуется указать на вкладке **Внешний вид**.

Описание параметров

Параметр	Описание
Имя	Название виджета.
Описание	Описание виджета.
Цвет	Цвет отображения информации: • **по умолчанию** – цвет шрифта, который используется в вашем браузере по умолчанию; • **зеленый;** • **красный;** • **синий;** • **желтый.**
Градиент	Градиентная заливка графика: • Двухцветная (красно-зеленая). • Трехцветная (красно-желто-зеленая). Параметр доступен для графиков типа Столбчатая диаграмма, Таблица. Вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Если границы градиента не заданы вручную, они рассчитываются автоматически по значениям данных. Если между заданными границами нет данных, градиент не применяется. Вместо него используется два цвета: один для значений ниже нижней границы, другой – для значений выше верхней.
Поле с индикатором градиента	Столбец, в котором отображаются маркеры градиентной заливки. Параметр доступен для графика типа **Таблица**.
Горизонтальный	Использование горизонтальной гистограммы вместо вертикальной. При включении этого параметра вся имеющаяся информация будет отражена в заданном размере виджета. Если данных много, вы можете увеличить размер виджета для оптимального отображения.
Итоговые значения	Суммы значений.

Параметр	Описание
Легенда	Отображение легенды для аналитики. По умолчанию переключатель включен.
Пустые значения в легенде	Отображение параметров с нулевым значением в легенде для аналитики. По умолчанию переключатель включен. Пустые значения отображаются только при включенном параметре **Показать данные за предыдущий период**, если в текущем периоде данных нет, а в предыдущем были.

Виджет Контекстные таблицы

Вы можете использовать виджет **Контекстные таблицы** для получения аналитики на основе SQL-запросов.

При создании этого виджета вам требуется указать значения для следующих параметров:

Вкладка Общие

В таблице ниже описаны параметры, значение которых требуется указать на вкладке **Общие**.

Описание параметров

Параметр	Описание
График	Доступны следующие типы графиков: • **Столбчатая диаграмма** • **Круговая диаграмма** • **Счетчик** • **Таблица**
Коррелятор	Название коррелятора, содержащего контекстную таблицу, по которой вы хотите получать данные.
Контекстная таблица	Название контекстной таблицы, по которой вы хотите получать данные. Одна и та же контекстная таблица может использоваться в разных корреляторах. При этом для каждого коррелятора создается своя сущность контекстной таблицы. Таким образом, содержимое контекстных таблиц, используемых разными корреляторами, различается, даже если идентификатор и название контекстных таблиц одинаковые.

Параметр	Описание
Поле SQL-запроса	В этом поле вы можете ввести запрос для фильтрации и поиска данных контекстной таблицы вручную. По умолчанию для каждого типа графика в поле указан запрос, который получает схему контекстной таблицы и ключ по ключевым полям. Структура запроса аналогична той, которая используется при поиске событий. При создании запроса по контекстным таблицам вам нужно учитывать следующие особенности: • Для функции `FROM` требуется указать значение `` `records` ``. • Вы можете получить данных только по полям, указанным в схеме контекстной таблицы. • Вы можете использовать поддерживаемые функции ClickHouse. • Если вы хотите получать данные по полям, названия которых содержат пробелы и символы кириллицы, в запросе такие названия требуется выделять кавычками: • В функции `SELECT` псевдонимы следует выделять двойными или косыми кавычками: `"<alias">`, `` `<another alias>` ``. • В функции `ORDER BY` псевдонимы следует выделять косыми кавычками: `` `<another alias>` ``. • Значения полей событий выделяются прямыми кавычками: `WHERE DeviceProduct = 'Microsoft'`. • Название полей событий выделять кавычками не требуется. • Если название поля активного листа начинается или заканчивается пробелами, в виджете эти пробелы не отображаются. Название поля не должно состоять только из пробелов. • Если значения полей активного листа могут содержать пробелы в конце или в начале, поиск по ним рекомендуется осуществлять с помощью функции `LIKE '%<field value>%'`. • Вы можете использовать в запросе служебное поле `_count` (сколько раз эта запись была добавлена в контекстную таблицу), а также пользовательские поля. • Псевдонимы `metric` и `value` в SQL-запросах недоступны для изменения для всех типов виджета с аналитикой по активным листам, кроме таблиц. • Если в SQL-запросе используется функция преобразования даты и времени (например, `fromUnixTimestamp64Milli`) и при этом обрабатываемое поле не содержит даты и времени, в виджете будет отображаться ошибка. Чтобы избежать этого, используйте функции, которые могут обрабатывать нулевое значение. Например: `SELECT _key, fromUnixTimestamp64Milli(toInt64OrNull(DateTime)) as Date FROM `records` LIMIT 250`. • Если задать большие значения для функции `LIMIT`, это может привести к ошибкам в работе браузера. • Если в качестве типа графика вы выбрали **Счетчик**, необходимо для значений функции `SELECT` указывать способ обработки данных: `count`, `max`, `min`, `avg`, `sum`. • В виджетах с графиком типа **Таблица** градиент доступен только для полей типа **INT**, **FLOAT** и для поля **_count**. Поле можно выбрать в раскрывающемся списке **Поле с индикатором градиента**. После этого ячейки выбранного столбца будут подсвечены маркерами градиентной заливки. Особенности использования псевдонимов в SQL-функциях и `SELECT`: допустимо использовать двойные и косые кавычки: ", `. При использовании пробелов или кириллицы псевдоним необходимо выделять кавычками: `"<Alias with a space>"`, Значения следует выделять прямыми одинарными кавычками: `'<Value with a space>'`. При отображении данных за предыдущий период сортировка по параметру count(ID) может работать некорректно. Рекомендуется использовать сортировку по параметру `metric`. Например, `SELECT count(ID) AS "metric", Name AS "value" FROM `events` GROUP BY Name ORDER BY metric ASC LIMIT 250`.

Примеры запросов для получения аналитики по активным листам:

- `SELECT * FROM `records` WHERE "Источник событий" = 'Екатеринбург' LIMIT 250`
  Запрос, который возвращает ключ активного листа с названием поля `"Источник событий"` и значением этого поля `"Екатеринбург"`.
- `SELECT count(_key) AS metric, Status AS value FROM `records` GROUP BY value ORDER BY metric DESC LIMIT 250`
  Запрос для круговой диаграммы, который возвращает количество ключей активного листа (агрегация `count` по полю **_key**) и все варианты значений пользовательского поля Status. В виджете отображается круговая диаграмма с общим количеством записей активного листа, пропорционально разделенным на количество вариантов значений поля **Status**.
- `SELECT Name, Status, _count AS Number FROM `records` WHERE Description ILIKE '%ftp%' ORDER BY Name DESC LIMIT 250`
  Запрос для таблицы, которая возвращает значения пользовательских полей **Name** и **Status**, а также служебного поля **_count** у тех записей активного листа, в которых значения пользовательского поля Description соответствует запросу `ILIKE '%ftp%'`. В виджете отображается таблица со столбцами **Status**, **Name** и **Number**.

Вкладка Оси

В таблице ниже описаны параметры, значение которых требуется указать на вкладке **Оси**.

Вкладка отображается, если на вкладке **Общие** в поле **График** вы выбрали значение **Столбчатая диаграмма**.

Описание параметров

Параметр	Описание
Ось Y и **Мин - Макс**	Масштаб оси Y. На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.
Ось X и **Мин - Макс**	Масштаб оси X. На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.

Вкладка Внешний вид

В таблице ниже описаны параметры, значение которых требуется указать на вкладке **Внешний вид**.

Описание параметров

Settings	Описание
Имя	Название виджета.
Описание	Описание виджета.
Цвет	Цвет отображения информации: • **по умолчанию** – цвет шрифта, который используется в вашем браузере по умолчанию; • **зеленый;** • **красный;** • **синий;** • **желтый.**
Градиент	Градиентная заливка графика: • Двухцветная (красно-зеленая). • Трехцветная (красно-желто-зеленая). Параметр доступен для графиков типа **Столбчатая диаграмма**, **Таблицы**. Вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Если границы градиента не заданы вручную, они рассчитываются автоматически по значениям данных. Если между заданными границами нет данных, градиент не применяется. Вместо него используется два цвета: один для значений ниже нижней границы, другой – для значений выше верхней.
Поле с индикатором градиента	Столбец, в котором отображаются маркеры градиентной заливки. Параметр доступен для графика типа **Таблица**.
Горизонтальный	Использование горизонтальной гистограммы вместо вертикальной. При включении этого параметра вся имеющаяся информация будет отражена в заданном размере виджета. Если данных много, вы можете увеличить размер виджета для оптимального отображения.
Итоговые значения	Суммы значений.
Легенда	Отображение легенды для аналитики. По умолчанию переключатель включен.
Пустые значения в легенде	Отображение параметров с нулевым значением в легенде для аналитики. По умолчанию переключатель включен. Пустые значения отображаются только при включенном параметре **Показать данные за предыдущий период**, если в текущем периоде данных нет, а в предыдущем были.

Пользовательский виджет Активы

Вы можете использовать виджет **Активы → Пользовательский виджет** для получения расширенной аналитики по активам из обработанных событий с помощью конструктора запросов. В запросе необходимо указать поле актива и соответствующее ему условие или набор условий, по которым должен вестись подсчет активов (ось Y). Также вы можете указать одно или несколько дополнительных условий (категорий), по которым будет производиться сравнение количества активов для каждого поля.

При создании пользовательского виджета активов вам требуется указать значения для параметров, описанных в таблицах ниже.

Вкладка Общие

В таблице ниже описаны параметры, расположенные на вкладке **Общие**.

Описание параметров

Параметр	Описание
Название	Название виджета. При сохранении отчета в формате Excel название виджета, отображаемое в заголовке листа, ограничено 31 символом. Рекомендуется называть виджеты с учетом этого ограничения.
График	Тип графика. Доступны следующие типы графиков: • **Круговая диаграмма**. Отображается распределение активов по указанным категориям для всех выбранных тенантов. • **Счетчик**. Подсчет активов выполняется только по одному условию. На диаграмме отображается сумма активов, соответствующих условию, по всем выбранным тенантам. • **Таблица**. Подсчет активов выполняется по указанным категориям по всем выбранным тенантам. Каждой категории на диаграмме соответствует отдельная строка. Название категории отображается в столбце **value**. Количество активов, соответствующих условию, отображается в столбце **metric**. • **Столбчатая диаграмма с накоплением**. Подсчет активов выполняется по указанным категориям по всем выбранным тенантам с возможностью группировки по тенантам (в этом случае отдельные тенанты располагаются по оси X). Каждой категории соответствует своя область на столбцах диаграммы, выделенная отдельным цветом. Названия категорий отображаются в легенде. С помощью флажков слева от названий категорий можно скрыть или показать соответствующие области на столбцах. • **Спидометр**. Подсчет активов выполняет с помощью соотношения количества активов, удовлетворяющих указанному условию, и общего количества активов. Значения на графике указываются в процентах.
Формат	Параметр доступен для графика типа **Столбчатая диаграмма с накоплением**. Формат отображения данных: **Абсолютные значения** или **Относительные значения, %**. При выборе формата **Абсолютные значения** высота столбцов диаграммы соответствует сумме значений измеряемого показателя. При выборе формата **Относительные значения, %** все столбцы имеют одинаковую высоту 100%, а размеры цветных областей столбца соответствуют процентному соотношению между значениями показателя. По умолчанию выбрано **Абсолютные значения**.
Тенант	Тенант, по которому отображаются данные на виджете. Вы можете выбрать несколько тенантов. По умолчанию данные отображаются по тенантам, которые вы выбрали в параметрах макета.
Категория активов	Категория активов, для которой отображаются данные на виджете.
Искать в активах без категории	Параметр позволяет отображать активы без категории. По умолчанию флажок не установлен.
Группа параметров **Выбор осей графика**	
Ось Y	Обязательный параметр. Поле актива и указанное для этого поля условие или набор условий, по которым должен вестись подсчет активов.
Категория оси Y	Категория для выбранного поля. Не используется для графика типа **Счетчик**. Параметр является необязательным для полей оси Y, значения которых являются перечислением (могут выбираться из конечного списка значений). Для всех остальных полей параметр является обязательным.
Группировка по тенантам	Параметр доступен для графика типа **Столбчатая диаграмма с накоплением**. Задает дополнительную группировку активов по тенантам. Если флажок установлен, активы на диаграмме разбиваются по оси X на столбцы, соответствующие отдельным тенантам. Если флажок не установлен, все активы отображаются на одном столбце. По умолчанию флажок не установлен.

Вкладка Внешний вид.

В таблице ниже описаны параметры, расположенные на вкладке **Внешний вид**.

Параметр	Описание
Описание	Описание виджета.
Итоговые значения	Параметр доступен для графика типа **Круговая диаграмма**. Включает отображение итоговых значений на диаграмме, помимо выбранных категорий. Если переключатель включен, сумма значений всех указанных категорий отображается в центре круговой диаграммы и в легенде в отдельной графе **Всего**. По умолчанию переключатель выключен.
Цвет	Параметр доступен для графика типа **Счетчик**. Цвет отображения информации: • **по умолчанию** – цвет шрифта, который используется в вашем браузере по умолчанию; • **зеленый**; • **красный**; • **синий**; • **желтый**.
Градиент	Градиентная заливка графика: • двухцветная (красно-зеленая); • трехцветная (красно-желто-зеленая). Параметр доступен для графика типа **Таблица**. Вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Если границы градиента не заданы вручную, они рассчитываются автоматически по значениям данных. Если между заданными границами нет данных, градиент не применяется. Вместо него используется два цвета: один для значений ниже нижней границы, другой – для значений выше верхней.
Поле с индикатором градиента	Столбец, в котором будут отображаться маркеры градиентной заливки. Этот столбец определяется полем **Metric**, выбранном в раскрывающемся списке. Параметр доступен для графика типа **Таблица**.
Горизонтальный	Использование горизонтальной гистограммы вместо вертикальной. При включении этого параметра горизонтальная прокрутка при большом количестве данных не будет отображаться и вся имеющаяся информация будет отражена в заданном размере виджета. Если данных для отображения много, рекомендуется увеличить размер виджета.
Легенда	Отображение легенды для аналитики. По умолчанию переключатель включен.
Пустые значения в легенде	Отображение параметров с нулевым значением в легенде для аналитики. По умолчанию переключатель включен. Пустые значения отображаются только при включенном параметре **Показать данные за предыдущий период**, если в текущем периоде данных нет, а в предыдущем были.
Отображать проценты в легенде	Отображение процентных значений в легенде. По умолчанию переключатель включен.
Десятичные знаки	Количество десятичных знаков, до которых отображаемое значение должно быть округлено.
Шкала	Доступно для графика типа **Столбчатая диаграмма с накоплением**. Шкала для отображения данных. Возможны следующие значения: • **Линейная**. • **Квадратичная**. • **Логарифмическая**. По умолчанию выбрано значение **Линейная**.
Пороговые значения	Доступно для графика типа **Спидометр**. По умолчанию установлены следующие интервалы значений: 0 - 30, 30 - 70, 70 - 100.

Виджет Изображение

Виджет позволяет разместить изображение на панели мониторинга или в отчете. Например, вы можете использовать виджет **Изображение** для оформления логотипа компании на панели мониторинга или в отчете.

У виджета **Изображение** отсутствует боковая панель с параметрами настройки.

Чтобы добавить файл изображения, наведите курсор на виджет и нажмите **Загрузить изображение**, в появившемся окне файловой системы выберите нужный файл, после добавления файла в виджет нажмите **Сохранить**.

Вы можете добавить несколько виджетов **Изображение** на панель мониторинга. Путем удержания кнопки ( ) и перетаскивания можно переместить виджеты по панели мониторинга и расположить виджеты в желаемом порядке.

Вы можете создать панель мониторинга с виджетом **Изображение** без добавления файла изображения, например, для разметки. Kaspersky SIEM Cloud сохранит панель мониторинга, а затем вы можете редактировать панель мониторинга с помощью кнопки **Изменить** на панели инструментов, и добавить файлы изображения.

Минимальные размеры виджета: 225x161 пикселей. Максимальные размеры: 465x692 пикселей. С помощью кнопки ( ) вы можете изменять размер изображения на виджете. При изменении размеров изображение не обрезается, а масштабируется относительно размеров виджета.

Максимальный размер файла изображения: 3 МБ.

Поддерживаемые форматы файлов изображения: xbm, tif, pjp, apng, svgz, jpg, jpeg, heif, ico, tiff, webp, jfif, heic, gif, svg, png, bmp, pjpeg, avif.

Скачивание данных виджетов в формате CSV не поддерживается.

Вы можете создать, редактировать, дублировать, удалить виджет.
Виджет Текст
Виджет позволяет разместить произвольный текст на панели мониторинга или в отчете. Например, виджет **Текст** можно использовать для отображения названия или краткого описания панели мониторинга или отчета.

Чтобы добавить или изменить текст, нажмите на виджет. При этом активируется поле ввода и появляется панель, позволяющая отформатировать введенный текст. Вы можете ввести до 2000 символов.

У виджета **Текст** отсутствует боковая панель с параметрами настройки. Такой виджет нельзя выгрузить в формат CSV.

Другие виджеты
В этом разделе описываются параметры всех виджетов, кроме виджетов **События**, **Активные листы**, **Контекстные таблицы** и пользовательский виджет **Активы**.

Набор параметров, доступных для виджета, зависит от типа графика, который отображается на виджете. В Kaspersky SIEM Cloud доступны следующие типы графиков:

- Круговая диаграмма ( ).
- Счетчик ( ).
- Таблица ( ).
- Столбчатая диаграмма ( ).
- Календарная диаграмма ( ).
- Линейная диаграмма.
- Сложенная столбчатая диаграмма.
- Спидометр.

Параметры для круговых диаграмм

В таблице ниже представлены параметры для графиков типа **Круговая диаграмма**.

Описание параметров

Параметр	Описание
Имя	Название виджета.
Описание	Описание виджета.
Период	Период, за который отображаются данные на виджете. По умолчанию выбрано **Как на макете** – отображаются данные за период, выбранный для макета. Вы также можете указать период для виджета одним из следующих способов: • Выбрать точные дату и время начала и окончания периода в календаре и нажать на кнопку **Применить**. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: выбрать точные дату и время или относительный период либо использовать комбинацию этих способов. Подробнее см. ниже в подразделе *Настройка значения периода*.
Итоговые значения	Суммы значений.
Легенда	Отображение легенды для аналитики. По умолчанию переключатель включен.
Пустые значения в легенде	Отображение параметров с нулевым значением в легенде для аналитики. По умолчанию переключатель включен.
Десятичные знаки	Количество десятичных знаков, до которых отображаемое значение должно быть округлено.

Параметры для счетчиков

В таблице ниже представлены параметры для графиков типа **Счетчик**.

Описание параметров

Параметр	Описание
Имя	Название виджета.
Описание	Описание виджета.
Период	Период, за который отображаются данные на виджете. По умолчанию выбрано **Как на макете** – отображаются данные за период, выбранный для макета. Вы также можете указать период для виджета одним из следующих способов: • Выбрать точные дату и время начала и окончания периода в календаре и нажать на кнопку **Применить**. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: выбрать точные дату и время или относительный период либо использовать комбинацию этих способов. Подробнее см. ниже в подразделе *Настройка значения периода*.

Параметры для таблиц

В таблице ниже представлены параметры для графиков типа **Таблица**.

Описание параметров

Параметр	Описание
Имя	Название виджета.
Описание	Описание виджета.
Период	Период, за который отображаются данные на виджете. По умолчанию выбрано **Как на макете** – отображаются данные за период, выбранный для макета. Вы также можете указать период для виджета одним из следующих способов: • Выбрать точные дату и время начала и окончания периода в календаре и нажать на кнопку **Применить**. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: выбрать точные дату и время или относительный период либо использовать комбинацию этих способов. Подробнее см. ниже в подразделе *Настройка значения периода*.
Градиент	Градиентная заливка графика: • двухцветная (красно-зеленая); • трехцветная (красно-желто-зеленая). Вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Если границы градиента не заданы вручную, они рассчитываются автоматически по значениям данных. Если между заданными границами нет данных, градиент не применяется. Вместо него используется два цвета: один для значений ниже нижней границы, другой – для значений выше верхней.
Поле с индикатором градиента	Столбец, в котором отображаются маркеры градиентной заливки. Этот столбец определяется полем, выбранным в раскрывающемся списке. Тип поля зависит от типа виджета: • **Затронутые активы** – поле **Frequency**. • **Активы в инцидентах**, **Расширенный статус постоянной защиты активов из KSC**, **Пользователи в инцидентах** – поле **Count**.
Десятичные знаки	Количество десятичных знаков, до которых отображаемое значение должно быть округлено.

Параметры для столбчатых и календарных диаграмм

В таблице ниже представлены параметры для графиков типа **Столбчатая диаграмма** и **Календарная диаграмма**, расположенные на вкладке **Оси**.

Описание параметров

Параметр	Описание
Ось Y и **Мин - Макс**	Масштаб оси Y. На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.
Ось X и **Мин - Макс**	Масштаб оси X. На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.
Десятичные знаки	Количество десятичных знаков, до которых отображаемое значение должно быть округлено.

В таблице ниже представлены параметры для графиков типа **Столбчатая диаграмма**, **Сложенная столбчатая диаграмма** и **Календарная диаграмма**, расположенные на вкладке **Внешний вид**.

Описание параметров

Параметр	Описание
Имя	Название виджета.
Описание	Описание виджета.

Параметр	Описание
Период	Период, за который отображаются данные на виджете. По умолчанию выбрано **Как на макете** – отображаются данные за период, выбранный для макета. Вы также можете указать период для виджета одним из следующих способов: • Выбрать точные дату и время начала и окончания периода в календаре и нажать на кнопку **Применить**. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: выбрать точные дату и время или относительный период либо использовать комбинацию этих способов. Подробнее см. ниже в подразделе *Настройка значения периода*.
Формат	Формат отображения данных: **Абсолютные значения** или **Относительные значения, %**. Параметр доступен для графика типа **Сложенная столбчатая диаграмма**. При выборе формата **Абсолютные значения** высота столбцов диаграммы соответствует сумме значений измеряемого показателя. При выборе формата **Относительные значения, %** все столбцы имеют одинаковую высоту 100%, а размеры цветных областей столбца соответствуют процентному соотношению между значениями показателя. По умолчанию выбрано **Абсолютные значения**.
Вид временной диаграммы	Формат отображения временных данных: **Столбчатая диаграмма** или **Линейная диаграмма**. Параметр доступен для графика типа **Календарная диаграмма**. При выборе формата **Столбчатая диаграмма** данные по умолчанию отображаются в виде вертикальных столбцов. Если SQL-запрос содержит дополнительное поле с псевдонимом `category`, столбчатая диаграмма будет представлена в виде сложенной диаграммы, то есть с разбивкой каждого столбца по значениям этого поля. При выборе формата **Линейная диаграмма** данные отображаются в виде одной или нескольких (в зависимости от запроса) ломаных линий, соединяющих точки на временной оси. По умолчанию выбран формат **Столбчатая диаграмма**.
Показывать данные за предыдущий период	Включение отображения данных сразу за два периода: текущий и предыдущий.
Цвет	Цвет отображения информации: • **по умолчанию** – цвет шрифта, который используется в вашем браузере по умолчанию; • **зеленый**; • **красный**; • **синий**; • **желтый**.
Градиент	Градиентная заливка графика: • двухцветная (красно-зеленая); • трехцветная (красно-желто-зеленая). Вы можете настроить направление заливки, нажав на значок переключения направления (⇆), а также задать пороговые значения. Если границы градиента не заданы вручную, они рассчитываются автоматически по значениям данных. Если между заданными границами нет данных, градиент не применяется. Вместо него используется два цвета: один для значений ниже нижней границы, другой – для значений выше верхней.Градиентная заливка не применяется для сложенных столбчатых диаграмм. В этом случае цвета назначаются автоматически.
Горизонтальный	Использование горизонтальной гистограммы вместо вертикальной. При включении этого параметра вся имеющаяся информация будет отражена в заданном размере виджета. Если данных много, вы можете увеличить размер виджета для оптимального отображения.
Итоговые значения	Суммы значений.
Легенда	Отображение легенды для аналитики. По умолчанию переключатель включен.
Пустые значения в легенде	Отображение параметров с нулевым значением в легенде для аналитики. По умолчанию переключатель включен. Пустые значения отображаются только при включенном параметре **Показать данные за предыдущий период**, если в текущем периоде данных нет, а в предыдущем были.
Длительность отрезков периода	Продолжительность сегментов, на которые вы хотите разделить период. Доступно для графиков типа **Календарная диаграмма**.

Параметры для графиков типа Спидометр

В таблице ниже представлены параметры для графика **Спидометр**.

> Значения на графике указываются в процентах.

Описание параметров

Параметр	Описание
Вкладка **Общие**	
Имя	Название виджета.
Категория активов	Активы выбранной категории, по которым будет осуществляться поиск значений.
Искать в активах без категории	Поиск активов для формирования графика осуществляется без учета категорий активов.
Ось Y	Указывается значение параметра, по которому будет выполнятся поиск активов и дальнейшее вычисление показания спидометра. Вы можете указать несколько значений параметров для поиска активов.
Вкладка **Внешний вид**	
Описание	Описание графика, которое отображается на виджете.
Предел событий	Для визуального определения критичности события циферблат спидометра разделен на три области: зеленую, желтую и красную. По умолчанию для этих областей определены следующие интервалы: • зеленый: 0–30; • желтый: 30–70; • красный: 70–100. При необходимости вы можете изменить интервалы значений.

Настройка значения периода

Для таких графиков, как **Круговая диаграмма**, **Счетчик**, **Таблица**, **Столбчатая диаграмма**, **Сложенная столбчатая диаграмма**, **Календарная диаграмма**, вы можете настроить период отображения данных в виджете с помощью параметра **Период**. По умолчанию период отображения данных виджета совпадает с периодом отображения данных панели мониторинга.

Чтобы настроить период отображения данных, выполните одно из следующих действий:

- При необходимости измените дату и время в параметре **Период** одним из следующих способов:

  - Если вы хотите указать точную дату, в календаре слева выберите даты начала и окончания периода и нажмите на кнопку **Применить**.

    Вы можете выбрать дату до текущей включительно. Формат даты и времени зависит от параметров вашего браузера. Если в поле **Дата от** или **Дата до** есть значение и вы не меняли вручную значение времени, при выборе даты в календаре в поле **Дата от** автоматически подставится время 00:00:00.000, а в поле **Дата до** – 23:59:59.999. Если вы вручную удалили значение в поле **Дата от** или **Дата до**, при выборе даты в календаре в поле автоматически подставится текущее время. После того как вы выберите значение в одном из полей, фокус переключается на другое поле. Если в поле **Дата до** вы выбираете значение, которое меньше значения в поле **Дата от**, это меньшее значение будет автоматически подставлено в поле **Дата от**.

- Если вы хотите указать относительный период, выберите один из доступных периодов в списке **Относительный период** справа.

  Период рассчитывается относительно настоящего времени.

- Если вы хотите задать пользовательский период, укажите или измените значение вручную в полях **Дата от** и **Дата до**.

  Вы можете указать точные дату и время в формате **DD.MM.YYYY HH:mm:ss.SSS** для русской локализации и **YYYY-MM-DD HH:mm:ss.SSS** для английской локализации или период относительно текущего времени в виде формулы. При необходимости вы также можете комбинировать эти способы. Если при вводе точной даты вы не указали миллисекунды, значение 000 подставляется автоматически. Если вы вручную изменили время в полях **Дата от** или **Дата до**, при переключении даты в календаре значение времени не меняется.

  В формулах относительного периода используйте параметр **now** для обозначения текущих даты и времени, а также: символы "+" (только в поле **Дата до**), "-", "/" (округление до ближайшего) и единицы изменения времени **y** (год), **M** (месяц), **w** (неделя), **d** (день), **h** (час), **m** (минута), **s** (секунда). Например, вы можете указать период **now-5d**, чтобы получить данные за последние пять дней, или **now/w**, чтобы получить данные с начала первого дня текущей недели (00:00:00:000 в UTC) до текущего времени **now**.

  > Поле **Дата от** является обязательным, и его значение не может превышать значение, установленное в поле **Дата до**, а также не может быть меньше 01.01.1970 (при указании точной даты или относительного периода). Значение в поле **Дата до** не должно быть меньше значения, установленного в поле **Дата от**. Если вы не укажете значение в поле **Дата до**, параметр **now** указывается автоматически.

Время в KUMA хранится в UTC, но в интерфейсе оно конвертируется в соответствии с часовым поясом вашего браузера. Это нужно учитывать для относительных периодов **Сегодня**, **Вчера**, **Эта неделя** и **Этот месяц**. Например, если в браузере установлен часовой пояс UTC+3 и вы выбрали период отображения данных **Сегодня**, данные будут отображаться за период с 03:00:00.000 до текущего времени, а не с 00:00:00.000.

Если при выборе относительного периода **Сегодня**, **Вчера**, **Эта неделя** или **Этот месяц** вы хотите отобразить данные в соответствии с вашим часовым поясом, вам нужно вручную добавить сдвиг по времени в поля **Дата от** и **Дата до** (если указано значение кроме now), прибавив или убавив необходимое количество часов. Например, если в браузере установлен часовой пояс UTC+3 и вы хотите отобразить данные за период **Вчера**, вам нужно изменить значение в поле **Дата от** на **now-1d/d-3h**, а в поле **Дата до** – на **now/d-3h**. Если же вы хотите отобразить данные за период **Сегодня**, вам нужно изменить значение только в поле **Дата от** на **now/d-3h**.

> Если вам нужны результаты до 23:59:59:999 вчерашнего дня в UTC, то используйте SQL-запрос с фильтром по Timestamp или укажите точные дату и время.

Границы периода включаются: например, для периода **Сегодня** отобразятся события с начала сегодняшнего дня 00:00:00:000 UTC до текущего времени **now** включительно, а для периода **Вчера** – с начала вчерашнего дня 00:00:00:000 UTC до 00:00:00:000 UTC сегодняшнего дня. Вы можете посмотреть дату и время последнего обновления данных и точный период, за который отображаются данные, наведя курсор на значок периода на виджете.

Если параметр Показать данные за предыдущий период включен в свойствах виджета и виджет отображает данные за относительный период, во всплывающей подсказке также отображается предыдущий период. Предыдущий период рассчитывается относительно текущего периода – из начального и конечного значения текущего периода вычитается продолжительности текущего периода. Например, если данные обновляются ежедневно и отображаются за месяц, но прошли только первые 10 дней месяца, прошлым периодом будут считаться последние 10 дней прошлого месяца.

- Если вы хотите отобразить на виджете данные за период, выбранный для макета, вы можете нажать на

кнопку **Сбросить**. При изменении периода отображения данных на макете, также изменится отображаемый на виджете период.

Фильтрация данных на виджетах

Kaspersky SIEM Cloud позволяет вам фильтровать данные на виджетах типа **События**, выбирая параметры фильтрации в панели мониторинга. Вы можете применять фильтрацию данных в следующих случаях:

- Фильтрация данных на одном виджете

  Для фильтрации данного типа вам нужно прописать одну или несколько локальных переменных в SQL-запросе в свойствах виджета. Переменные позволяют вам изменять этот SQL-запрос, подставляя в него данные, которые представлены на виджете в панели мониторинга. Виджет отфильтрует данные с учетом новых значений переменных и перестроит график. При этом вам не нужно вручную изменять SQL-запрос в свойствах виджета.

  Локальные переменные вы можете применить, нажав на значок воронки (▽) на виджете. В открывшемся окне вы сможете выбрать или ввести значения для локальных переменных.

- Фильтрация данных на нескольких виджетах в рамках одной панели мониторинга

  Для фильтрации данного типа вам нужно прописать одну или несколько глобальных переменных в свойствах панели мониторинга. Затем добавьте глобальные переменные в SQL-запросы виджетов, к которым хотите применять эти глобальные переменные. Когда вы присваиваете глобальной переменной новое значение, все виджеты, в которых эта переменная используется, автоматически перестраивают графики с учетом нового значения.

  Глобальные переменные применяются по щелчку кнопкой мыши на сегменте графика или на тексте из легенды графика. Kaspersky SIEM Cloud отобразит меню с командами, позволяющими применить категорию данных выбранного сегмента графика или значение элемента легенды графика к переменной.

- Переход в другую панель мониторинга с одновременной передачей параметров фильтрации

  Глобальные переменные можно использовать для передачи значений в другую панель мониторинга. При переходе из одной панели мониторинга в другую Kaspersky SIEM Cloud подставит выбранное значение переменной и выбранный временной период, а графики в новой панели автоматически перестроятся.

  Локальные переменные не могут быть использованы при переходе в другую панель мониторинга.

Не рекомендуется задавать более пяти переменных в рамках одной панели мониторинга. Это может привести к нестабильной работе панели мониторинга.

Фильтрация данных на одном виджете

Kaspersky SIEM Cloud позволяет вам фильтровать данные на виджетах типа **События**, выбирая параметры фильтрации в панели мониторинга.

Для фильтрации данных на одном виджете вам нужно прописать одну или несколько локальных переменных в SQL-запросе в свойствах виджета. Переменные позволяют вам изменять этот SQL-запрос, подставляя в него данные, которые представлены на виджете в панели мониторинга. Виджет отфильтрует данные с учетом новых значений переменных и перестроит график. При этом вам не нужно вручную изменять SQL-запрос в свойствах виджета.

Не рекомендуется задавать более пяти переменных в рамках одной панели мониторинга. Это может привести к нестабильной работе панели мониторинга.

Настройка фильтрации данных на одном виджете

Чтобы настроить локальные переменные для фильтрации данных в рамках одного виджета:

1. В разделе **Мониторинг** → **Панель мониторинга** → **Обнаружение и реагирование** выберите панель мониторинга и затем нажмите на кнопку **Изменить**, чтобы перейти в режим редактирования панели мониторинга.

2. Выберите существующий виджет **События** или нажмите на кнопку **Добавить виджет** и затем выберите тип виджета **События**.

3. В окне свойств виджета перейдите на вкладку **Общие**.

4. В блоке параметров **Доступные переменные** нажмите на кнопку **Добавить**.

5. Введите произвольное имя переменной, затем укажите значение переменной. Имена локальных и глобальных переменных должны быть уникальными в рамках панели мониторинга.

   В качестве значения переменной укажите `value` или `category`, то есть псевдонимы полей, используемые в запросе. Если хотите при фильтрации данных в виджете вводить значение этой переменной вручную, оставьте поле пустым.

   Для графиков типа таблица в качестве значения переменной вы можете указать название поля события. Тогда вы сможете фильтровать данные в таблице по выбранному значению этого поля. Название поля события будет отображаться в заголовке столбца таблицы.

6. В поле **SQL-запрос** в оператор WHERE добавьте функцию для работы с переменными.

   Синтаксис для переменных с конкретным значением:

   ```
   filter(<event_field_name> = $variable_name)
   ```

   Синтаксис для переменных с произвольным значением, которое задается вводом вручную:

   ```
   filter(<event_field_name> like $variable_name)
   ```

   В этом случае при вводе вручную вы можете использовать метасимвол % для поиска частичных текстовых совпадений. Подробную информацию смотрите в документации ClickHouse.

> Вы не можете использовать конструктор SQL для добавления переменных в SQL-запрос.

Посмотреть пример

Пример SQL-запроса с использованием локальной переменной

```
SELECT count(ID) AS 'metric', Name AS 'value', TenantID AS 'category' FROM 'events' WHERE filter(Name = $Name)
GROUP BY Name, TenantID ORDER BY metric DESC LIMIT 250
```

В этом запросе использована локальная переменная `$Name`. В эту переменную будет подставляться значение из поля события `Name`. Вы можете применить переменную, нажав на значок воронки ( ) на виджете. В открывшемся окне вы сможете выбрать значение для переменной. Виджет отфильтрует выборку по выбранному значению поля `Name`.

Обратите внимание, если в SQL-запросе вы указываете переменную для поля, которое принимает числовое значение, такое значение надо преобразовать в строку. Для этого используйте функцию `toString`. Иначе SQL-запрос вернет ошибку.

Пример

```
SELECT count(ID) AS `metric`, SourcePort AS `value` FROM `events` WHERE (filter(toString(SourcePort) like
$SourcePort)) GROUP BY SourcePort ORDER BY value ASC LIMIT 250
```

В этом запросе поле события `SourcePort` имеет числовое значение, поэтому оно преобразовано в строку `toString(SourcePort)`.

7. Сохраните изменения.

Применение фильтрации данных на одном виджете

Чтобы применить локальную переменную для фильтрации данных в рамках одного виджета:

1. В разделе **Мониторинг → Панель мониторинга → Обнаружение и реагирование** выберите панель мониторинга, на которой расположен требуемый виджет. В свойствах этого виджета должна быть задана хотя бы одна локальная переменная.

2. На виджете нажмите на значок воронки ( ).

3. В открывшемся окне выберите, какие локальные переменные вы хотите применить.

4. Сохраните изменения.

   Виджет перестроит график с учетом нового значения переменной.

Фильтрация данных на нескольких виджетах

Kaspersky SIEM Cloud позволяет вам фильтровать данные на виджетах типа **События**, выбирая параметры фильтрации в панели мониторинга.

Для фильтрации данных на нескольких виджетах в рамках одной панели мониторинга вам нужно прописать одну или несколько глобальных переменных в свойствах панели мониторинга. Затем добавьте глобальные переменные в SQL-запросы виджетов, к которым хотите применять эти глобальные переменные. Когда вы присваиваете глобальной переменной новое значение, все виджеты, в которых эта переменная используется, автоматически перестраивают графики с учетом нового значения.

Глобальные переменные применяются по щелчку кнопкой мыши на сегменте графика или на тексте из легенды графика. Kaspersky SIEM Cloud отобразит меню с командами, позволяющими применить категорию данных выбранного сегмента графика или значение элемента легенды графика к переменной.

Не рекомендуется задавать более пяти переменных в рамках одной панели мониторинга. Это может привести к нестабильной работе панели мониторинга.

Настройка фильтрации данных на нескольких виджетах на уровне панели мониторинга

Чтобы настроить глобальные переменные для фильтрации данных на уровне панели мониторинга:

1. В разделе **Мониторинг → Панель мониторинга → Обнаружение и реагирование** выберите панель мониторинга и затем нажмите на кнопку **Изменить**, чтобы перейти в режим редактирования панели мониторинга.

2. Нажмите на кнопку **Настройки**.

3. В открывшемся окне в разделе **Переменные** перейдите на вкладку **Глобальные переменные**.

4. Нажмите на кнопку **Добавить**.

5. В добавленную строку введите имя переменной. Имена локальных и глобальных переменных должны быть уникальными в рамках панели мониторинга.

   Названия всех виджетов панели мониторинга, в которые вы добавите глобальные переменные, будут перечислены в столбце **Используется в виджетах**.

   Имена глобальных переменных будет отображаться в командах контекстного меню виджета по щелчку на сегменте графика или на элементе легенды графика.

6. Сохраните изменения.

7. Выберите существующий виджет **События** или нажмите на кнопку **Добавить виджет** и затем выберите тип виджета **События**. В этом виджете настройте действия по нажатию на кнопку мыши.

8. В окне свойств виджета перейдите на вкладку **Общие**.

9. В разделе **Доступные переменные** добавьте одну или несколько глобальных переменных, которые вы добавили в свойствах панели мониторинга.

10. Если необходимо, в поле SQL-запроса добавьте глобальные переменные в оператор WHERE с помощью функции filter. В этом случае настраиваемые действия будут также применяться и к этому виджету.

11. Перейдите на вкладку **Действия**.

    Если вы хотите, чтобы при щелчке на сегменте графика отображалось меню с командой для фильтрации данных по выбранной категории сегмента:

    a. В разделе **Сегмент графика** включите параметр **Фильтровать по переменной**.

    b. В списке **Категория** выберите переменную, в которую вы хотите иметь возможность подставлять значение псевдонима `category`, указанного в SQL-запросе.

       Параметр **Категория** доступен только для типа графика сложенная столбчатая диаграмма.

    c. В списке **Значение** выберите переменную, в которую вы хотите иметь возможность подставлять значение псевдонима `value`, указанного в SQL-запросе.

Если вы хотите, чтобы при щелчке на элементе легенды графика отображалось меню с командой для фильтрации данных по выбранному значению:

a. В разделе **Элемент легенды** включите параметр **Фильтровать по переменной**.

   При необходимости нажмите на кнопку **Скопировать из параметров сегмента графика**, чтобы автоматически перенести выбранные значения параметров из блока параметров **Сегмент графика** в блок параметров **Элемент легенды**.

b. В списке **Значение** выберите переменные, в которые вы хотите иметь возможность подставлять значение элемента легенды.

12. В свойствах других виджетов, к которым вы хотите применять глобальные переменные:

- На вкладке **Общие** в разделе **Доступные переменные** добавьте одну или несколько глобальных переменных.
- В поле SQL-запроса виджета добавьте глобальные переменные в оператор WHERE с помощью функции filter.

Применение фильтрации данных на нескольких виджетах на уровне панели мониторинга

Чтобы применить глобальную переменную для фильтрации данных между виджетами:

1. В разделе **Мониторинг → Панель мониторинга → Обнаружение и реагирование** выберите панель мониторинга, к виджетам которой хотите применить глобальную переменную.
2. Найдите виджет, в свойствах которого прописаны действия по щелчку кнопкой мыши. Щелкните на сегменте графика или на значке стрелки (⌄) рядом с элементом легенды графика, чтобы открыть меню.
3. В меню нажмите **Применить категорию к переменной <имя переменной>** или **Применить значение к переменной <имя переменной>**.

   Переменная примет значение выбранной категории или выбранного элемента легенды. В рамках текущей панели мониторинга все виджеты, в которых используется эта переменная, перестроят графики с учетом нового значения переменной. Такие виджеты будут помечены значком воронки с цифрой, обозначающей количество примененных фильтров (1). В верхней части экрана появится список примененных глобальных переменных. Чтобы отменить фильтрацию данных для виджета, нажмите на значок воронки с цифрой (1). Чтобы отменить фильтрацию данных для всех виджетов панели мониторинга, нажмите **Сбросить все** в верхней части панели мониторинга.

Переход в связанную панель мониторинга

Kaspersky SIEM Cloud позволяет фильтровать данные на виджетах типа **События** в текущей панели мониторинга и переходить на другую панель мониторинга с сохранением настроенных параметров фильтрации и периода.

Для этого используются глобальные переменные. Они должны быть настроены в обеих панелях мониторинга, а также в свойствах виджетов: на целевой панели переменная указывается в SQL-запросе, а на исходной панели указывается при настройке параметра **Переход к другой панели мониторинга**. При переходе из одной панели мониторинга в другую Kaspersky SIEM Cloud автоматически подставляет выбранное значение переменной и период, после чего графики в целевой панели перестраиваются. Обе панели должны находиться в одном тенанте.

Локальные переменные не могут использоваться при переходе в другую панель мониторинга.

Настройка целевой панели мониторинга

Чтобы настроить целевую панель мониторинга:

1. В веб-консоли в разделе **Мониторинг → Панель мониторинга → Обнаружение и реагирование** выберите панель мониторинга и создайте глобальную переменную.

   Имя переменной должно содержать только английские буквы, цифры и не должно содержать пробелы.

2. Сохраните изменения.

3. В панели мониторинга выберите существующий виджет **События** или нажмите на кнопку **Добавить виджет** и затем выберите тип виджета **События**.

4. На вкладке **Общие** укажите созданную ранее переменную:

   - В блоке параметров **Доступные переменные**.
   - В поле **SQL-запрос**. Для того чтобы SQL-запрос учитывал значение переменной, добавьте в условие `WHERE` функцию `filter()`.

     Синтаксис для переменных с конкретным значением:

     ```
     filter(<event_field_name> = $variable_name)
     ```

     Синтаксис для переменных с произвольным значением, которое задается вручную:

     ```
     filter(<event_field_name> like $variable_name)
     ```

     Пример запроса

     Запрос с переменной `$ServiceName`:

     ```
     SELECT DestinationHostName AS Host, Name AS Status, Message AS Reason, ServiceName,
     Timestamp AS Time
     FROM events
     WHERE DeviceEventClassID = 'KLSRV_HOST_STATUS_CRITICAL' OR DeviceEventClassID =
     'KLSRV_HOST_STATUS_WARNING' AND filter(ServiceName = $ServiceName)
     ORDER BY Time DESC
     LIMIT 25
     ```

     Если при переходе в целевую панель мониторинга переменной `$ServiceName` передается значение, оно автоматически подставляется в запрос и данные фильтруются. Если значение переменной не задано, запрос выполняется так, как будто переменной в нем нет.

5. Сохраните изменения.

Настройка исходной панели мониторинга

Чтобы настроить исходную панель мониторинга:

1. В веб-консоли в разделе **Мониторинг → Панель мониторинга → Обнаружение и реагирование** выберите панель мониторинга и создайте глобальную переменную.

   Имя переменной должно совпадать с именем переменной, созданной на целевой панели. Имя должно содержать только английские буквы, цифры и не должно содержать пробелы.

2. Сохраните изменения.

3. В панели мониторинга выберите существующий виджет **События** или нажмите на кнопку **Добавить виджет** и затем выберите тип виджета **События**.

4. На вкладке **Общие** в блоке параметров **Доступные переменные** укажите созданную ранее переменную.

5. На вкладке **Действия** настройте следующие параметры:

   a. В разделе **Сегмент графика** или **Элемент легенды** включите параметр **Переход к другой панели мониторинга**.

   b. В раскрывающемся списке **Панели мониторинга** выберите целевую панель.

   c. В раскрывающемся списке **Значение** выберите переменную, значение которой будет передаваться при переходе. Это должна быть та же переменная, которую вы создали ранее.

      Выбранная переменная должна быть указана в SQL-запросе виджета целевой панели, чтобы данные на этом виджете автоматически были отфильтрованы после перехода.

6. Сохраните изменения.

Переход из исходной панели мониторинга в целевую панель мониторинга

Чтобы перейти в целевую панель мониторинга:

1. В веб-консоли в разделе **Мониторинг → Панель мониторинга → Обнаружение и реагирование** выберите исходную панель мониторинга.

2. Найдите виджет, в свойствах которого вы включили параметр **Переход к другой панели мониторинга**. Нажмите на сегмент или элемент легенды графика, для которых задано это действие.

   В новой вкладке откроется целевая панель мониторинга. При этом автоматически ко всей панели применится период исходного виджета, а выбранное значение в раскрывающемся списке **Значение** передастся как переменная в виджеты типа **События**, где эта переменная используется в SQL-запросе через функцию `filter()`. Графики в виджетах на другой панели перестроятся с учетом полученных параметров.

   > Если на целевой панели мониторинга, в которую выполняется переход, изменили или удалили переменную, которая указана в действии, переход будет выполняться, но значение переменной передаваться не будет.

Информационная панель Обнаружение и реагирование

В разделе **Панель мониторинга** вы можете контролировать состояние безопасности сети вашей организации.

Панель мониторинга представляет собой набор виджетов, которые отображают аналитику данных безопасности сети. Вы можете просматривать данные только для тех тенантов, к которым у вас есть доступ.

Набор виджетов, используемых в панели мониторинга, называется *макетом*. Вы можете создавать макеты вручную или воспользоваться преднастроенными макетами. Параметры виджетов в преднастроенных макетах можно редактировать при необходимости. По умолчанию в панели мониторинга отображается преднастроенный макет Alerts Overview.

Создавать, редактировать и удалять макеты могут только пользователи с ролями Главный администратор, Администратор тенанта, Аналитик 2-го уровня и Аналитик 1-го уровня. Пользователи с учетными записями всех ролей могут просматривать макеты и назначать макеты по умолчанию. Если макет назначен по умолчанию, этот макет отображается для учетной записи при каждом переходе в раздел **Панель мониторинга**. Выбранный макет по умолчанию сохраняется для текущей учетной записи пользователя.

Информация в панели мониторинга обновляется в соответствии с расписанием, заданным в параметрах макета. При необходимости вы можете обновить данные принудительно.

Для удобства представления данных в панели мониторинга вы можете включить режим ТВ. В этом случае вы перейдете в режим полноэкранного просмотра панели мониторинга в FullHD-разрешении. В режиме ТВ вы также можете настроить отображение слайд-шоу для выбранных макетов.
Создание макета панели мониторинга
Чтобы создать макет:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.

2. Откройте раскрывающийся список в правом верхнем углу окна и выберите **Создать макет**.

   Откроется окно **Новый макет**.

3. В раскрывающемся списке **Тенанты** выберите тенанты, которым будет принадлежать созданный макет и данные которых будут использоваться для заполнения виджетов макета.

   Выбор тенантов в этом раскрывающемся списке не имеет значения, если вы хотите создать универсальный макет (шаг 8).

4. В раскрывающемся списке **Период** выберите период, за который требуется аналитика:

   - **1 час**
   - **1 день** (это значение выбрано по умолчанию)
   - **7 дней**
   - **30 дней**
   - **За период** – получать аналитику за выбранный период. Период устанавливается с помощью календаря, который отображается при выборе этого параметра.

     Верхняя граница периода не входит в определяемый ею временной интервал. Другими словами, чтобы получать аналитику за 24-часовой период, вам нужно настроить период как День 1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.

5. В раскрывающемся списке **Обновлять каждые** выберите как часто нужно обновлять данные в виджетах макета:

   - **1 минута**
   - **5 минут**
   - **15 минут**

- **1 час** (это значение выбрано по умолчанию)
- **24 часа**

6. В раскрывающемся списке **Добавить виджет** выберите нужный виджет и настройте его параметры.

   В макет можно добавить несколько виджетов.

   Вы также можете перетаскивать виджеты по окну и изменять их размер с помощью диагональной кнопки (↘), которая появляется при наведении курсора мыши на виджет.

   Вы можете изменять или удалять виджеты, добавленные на макет. Для этого нажмите на значок параметров (⚙) и выберите пункт **Изменить**, чтобы изменить их конфигурацию, или пункт **Удалить**, чтобы удалить их из макета.

7. В поле **Имя макета** введите уникальное имя для этого макета. Имя должно содержать от 1 до 128 символов Юникода.

   Пользовательские панели мониторинга не могут иметь названия предустановленных панелей мониторинга.

   При попытке создать панель мониторинга с тем же именем, что и стандартная панель мониторинга, или сменить имя пользовательской панели мониторинга на имя предопределенной панели мониторинга в тенанте Main. В тенантах кроме Main нет ограничений по копированию или дублированию пользовательской панели мониторинга с тем же именем, что и у предопределенной панели мониторинга.

8. При необходимости нажмите на значок параметров (⚙) справа от поля названия макета и установите флажок рядом с параметром **Универсальные**.

   Виджеты макета будут отображать данные тенантов, которые вы выбрали в разделе **Выбранные тенанты** в меню слева. Это означает, что данные в виджетах макета будут изменяться в зависимости от выбранных вами тенантов без необходимости изменять параметры макета. Для универсальных макетов **тенанты**, выбранные в раскрывающемся списке, не учитываются.

   Если флажок снят, виджеты макета отображают данные от тенантов, выбранных в раскрывающемся списке **Тенанты** в параметрах макета. Если какой-либо из выбранных в макете тенантов недоступен для вас, их данные не будут отображаться в виджетах макета.

   > Вы не можете использовать виджет **Активные листы** в универсальных макетах.
   > Универсальные макеты может создавать и изменять только пользователь, которому назначена роль Главного администратора. Такие макеты могут просматривать все пользователи.

9. Нажмите на кнопку **Сохранить**.

Макет будет создан и отобразится на вкладке **Обнаружение и реагирования** в панели мониторинга.

Выбор макета панели мониторинга

Чтобы выбрать макет панели мониторинга:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Раскройте список в правом верхнем углу окна.
3. Выберите соответствующий макет.

Выбранный макет отображается на вкладке **Обнаружение и реагирование** в панели мониторинга.

Выбор макета панели мониторинга по умолчанию

Чтобы установить макет в панели мониторинга по умолчанию:

1. В главном окне приложения перейдите в раздел **Мониторинг → Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Раскройте список в правом верхнем углу окна.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на значок звездочка (☆).

Выбранный макет по умолчанию отображается на вкладке **Обнаружение и реагирование** в панели мониторинга.

Изменение макета панели мониторинга

Чтобы изменить макет панели мониторинга:

1. В главном окне приложения перейдите в раздел **Мониторинг → Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Раскройте список в правом верхнем углу окна.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на значок редактирования (✎).

   Откроется окно **Настройка макета**.
5. Измените макет панели мониторинга. Параметры, доступные для изменения, такие же, как и параметры, доступные при создании макета.
6. Нажмите на кнопку **Сохранить**.

Макет панели мониторинга изменен и отображается на вкладке **Обнаружение и реагирование**.

Если макет был удален или назначен другому тенанту во время его изменения, при нажатии на кнопку **Сохранить** отображается ошибка. Макет не сохранен. Обновите страницу интерфейса Kaspersky SIEM Cloud, чтобы увидеть список доступных макетов в раскрывающемся списке.

Удаление макета панели мониторинга

Чтобы удалить макет:

1. В главном окне приложения перейдите в раздел **Мониторинг → Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.
2. Раскройте список в правом верхнем углу окна.
3. Наведите курсор мыши на соответствующий макет.
4. Нажмите на значок удаления (🗑) и подтвердите это действие.

Макет удален.

Включение и отключение режима ТВ

Мы рекомендуем для отображения аналитики в режиме ТВ создать отдельного пользователя с минимально необходимым набором прав.

Чтобы включить режим ТВ:

1. В Консоли KUMA выберите раздел **Панель мониторинга**.
2. В правом верхнем углу нажмите на кнопку ⚙.

   Откроется окно **Параметры**.
3. Переведите переключатель **Режим ТВ** в положение **Включено**.
4. Чтобы настроить показ виджетов в режиме слайд-шоу:

   a. Переведите переключатель **Слайд-шоу** в положение **Включено**.

   b. В поле **Время ожидания** укажите, через сколько секунд должно происходить переключение макетов.

   c. В раскрывающемся списке **Очередь** выберите виджеты для просмотра. Если макет не выбран, в режиме слайд-шоу по очереди отображаются все доступные пользователю макеты.

   d. Если требуется, измените порядок показа макетов, перетащив их с помощью кнопки ⣿.
5. Нажмите на кнопку **Сохранить**.

Режим ТВ включен. Чтобы вернуться к работе с Консолью KUMA, нужно выключить режим ТВ.

Чтобы отключить режим ТВ:

1. В Консоли KUMA выберите раздел **Панель мониторинга**.
2. В правом верхнем углу нажмите на кнопку ⚙.

   Откроется окно **Параметры**.
3. Переведите переключатель **Режим ТВ** в положение **Выключено**.
4. Нажмите на кнопку **Сохранить**.

Режим ТВ выключен. В левой части экрана отобразится панель с разделами Консоли KUMA.

Когда вы вносите изменения в макеты, выбранные для слайд-шоу, эти изменения будут автоматически применены к активным сеансам слайд-шоу.

Преднастроенные макеты панели мониторинга

Kaspersky SIEM Cloud поставляется с набором преднастроенных макетов, которые содержат следующие виджеты:

- Макет **Alerts Overview** (Обзор алертов):
  - Active alerts (Активные алерты) – количество незакрытых алертов.
  - Неназначенные алерты – количество алертов, у которых нет исполнителя.
  - Latest alerts (Последние алерты) – таблица с информацией о последних 10 незакрытых алертах, принадлежащих выбранным в макете тенантам.
  - Alerts distribution (Распределение алертов) – количество алертов, созданных в течение указанного для виджета периода.
  - Alerts by priority (Алерты по приоритету) – количество незакрытых алертов, сгруппированных по приоритету.
  - Alerts by users (Алерты по пользователям) – количество алертов со статусом **В обработке**. Сгруппированы по имени учетной записи.
  - Alerts by status (Алерты по статусам) – количество алертов, сгруппированных по статусу.
  - Alerts by groups (Алерты по группам) – количество алертов, сгруппированных по группам пользователей.
  - Affected users in alerts (Пользователи в алертах) – пользователи, связанные с незакрытыми алертами.
  - Affected assets (Затронутые активы) – таблица с информацией об активах, их уровне важности и количестве связанных с ними незакрытых алертов. Уровень важности актива рассчитывается на основе категорий, к которым принадлежит актив, включая все родительские категории до корня иерархии.
  - Категории затронутых активов – диаграмма, на которой отображено количество категорий активов, указанных в незакрытых алертах и инцидентах. Для каждого актива, указанного в алертах и инцидентах, уровень важности рассчитывается на основе категорий, к которым принадлежит актив, включая все родительские категории до корня иерархии.
  - Топ источников событий по количеству алертов – количество незакрытых алертов, сгруппированных по источникам событий, который сгенерированы алертами.

    На виджете отображается не более 10 источников событий.

  - Alerts by rule (Алертов по правилу) – количество незакрытых алертов, сгруппированных по правилам корреляции.

Незакрытые алерты – это алерты, которые имеют один из следующих статусов: **Новый**, **В обработке**, **В инциденте**.

- Макет **Incidents Overview** (Обзор инцидентов):
  - Active incidents (Активные инциденты) – количество инцидентов, статусы которых отличны от **Завершен**.
  - Unassigned Incidents (Неназначенные инциденты) – количество инцидентов, у которых нет исполнителя.
  - Latest Incidents (Последние инциденты) – таблица с информацией о последних 10 незакрытых инцидентах, принадлежащих выбранным в макете тенантам.
  - Incidents distribution (Распределение инцидентов) – количество инцидентов, созданных в течение указанного для виджета периода.
  - Incidents by priority (Инциденты по приоритету) – количество незакрытых инцидентов, сгруппированных по приоритету.
  - Incidents by users (Инциденты по пользователям) – количество инцидентов со статусом **В обработке**. Сгруппированы по имени учетной записи пользователя.
  - Incidents by status (Инциденты по статусам) – количество инцидентов, сгруппированных по статусу.
  - Incidents by groups (Инциденты по группам) – количество незакрытых инцидентов, сгруппированных по группам пользователей.
  - Affected assets in incidents (Активы в инцидентах) – таблица с количеством активов, связанных с незакрытыми инцидентами. В таблице перечислены активы и их уровень важности – он рассчитывается на основе категорий, к которым принадлежит актив, вместе со всеми родительскими категориями до корня иерархии.
  - Affected users in incidents (Пользователи в инцидентах) – пользователи, связанные с незакрытыми инцидентами.
  - Affected asset categories in incidents (Категории затронутых активов в инцидентах) – график с количеством категорий активов, связанных с незакрытыми инцидентами. Для каждого актива, связанного с инцидентом, уровень важности рассчитывается на основе категорий, к которым принадлежит актив, включая все родительские категории до корня иерархии.
  - Active incidents by tenant (Инциденты по тенантам) – количество незакрытых инцидентов, сгруппированных по тенантам.

  Незакрытые инциденты – это инциденты, статусы которых отличны от **Завершен**.

- Макет **Network Overview** (Обзор сетевой активности):
  - Netflow top external IPs (Топ внешних IP-адресов по полученному netflow-трафику) – суммарный размер полученного активом netflow-трафика в байтах. Данные сгруппированы по внутренним IP-адресам активов.

    На виджете отображается не более 10 IP-адресов.
  - Netflow top external IPs (Топ внешних IP-адресов по полученному netflow-трафику) – суммарный размер полученного активом netflow-трафика в байтах. Данные сгруппированы по внешним IP-адресам активов.

- Netflow top hosts for remote control (Топ активов, на которые были обращения на порты для удаленного управления) – количество событий, связанных с обращением на один из следующих портов: 3389, 22, 135. Данные сгруппированы по именам активов.

- Netflow total bytes by internal ports (Топ внутренних портов по приему netflow-трафика) – количество байт, переданное на внутренние порты активов. Данные сгруппированы по номерам портов.

- Top Log Sources by Events count (Топ источников событий) – 10 источников, от которых было получено наибольшее количество событий.

- Макет **Агрегированные панели мониторинга NGFW**:

  - NGFW. Firewall Sessions & Actions (Сессии и действия сетевого экрана) – количество примененных действий разного типа в правилах фильтрации, для которых включено ведение журнала.

  - NGFW. DNS Security Sessions & Actions (Сессии и действия Защиты DNS-трафика) – количество примененных действий разного типа в профилях Защиты DNS-трафика, для которых включено ведение журнала.

  - NGFW. Web Control Sessions & Actions (Сессии и действия Веб-Контроля) – количество примененных действий разного типа в профилях Веб-Контроля, для которых включено ведение журнала.

  - NGFW. IDPS Sessions & Actions (Сессии и действия IDPS) – количество примененных действий разного типа в профилях IDPS, для которых включено ведение журнала.

  - NGFW. Anti-Virus Sessions & Actions (Сессии и действия Антивируса) – количество примененных действий разного типа в профилях Антивируса, для которых включено ведение журнала.

- Макет **NGFW IDPS & File Web Antivirus**:

  - NGFW. IDPS. Top-5 Threats Name (Топ 5 названий угроз) – пять угроз, чаще всего обнаруженных профилями IDPS.

  - NGFW. IDPS. Top-5 MITRE Tactics & Techniques (Топ 5 тактик и техник MITRE) – пять тактик и техник матрицы MITRE ATT&CK, чаще всего обнаруживаемых профилями IDPS.

  - NGFW. IDPS. Top-5 Threats Type (Топ 5 типов угроз) – пять типов угроз, чаще всего обнаруживаемых профилями IDPS.

  - NGFW. IDPS. Top-5 Destination IP Addresses With the Most Blocked Web Traffic (Топ 5 IP-адресов назначения с наибольшим объемом заблокированного веб-трафика) – пять IP-адресов назначения с наибольшим объемом трафика, заблокированного профилями IDPS.

  - NGFW. IDPS. Top-5 Source IP Addresses With the Most Blocked Web Traffic (Топ 5 IP-адресов источника с наибольшим объемом заблокированного веб-трафика) – пять IP-адресов источника с наибольшим объемом трафика, заблокированного профилями IDPS.

  - NGFW. File Web Antivirus. Top-5 Threats Name (Топ 5 названий угроз) – пять угроз, чаще всего обнаруживаемых профилями Антивируса.

- NGFW. File Web Antivirus. Top-5 Destination IP Addresses With the Most Blocked Web Traffic (Топ 5 IP-адресов назначения с наибольшим объемом заблокированного веб-трафика) – пять IP-адресов назначения с наибольшим объемом трафика, заблокированного профилями Антивируса.

- NGFW. File Web Antivirus. Top-5 Source IP Addresses With the Most Blocked Web Traffic (Топ 5 IP-адресов источника с наибольшим объемом заблокированного веб-трафика) – пять IP-адресов источника с наибольшим объемом трафика, заблокированного профилями Антивируса.

- Макет **NGFW DNS Security**:

  - NGFW. DNS Security. Top-5 Threats for Blocked Addresses (Топ 5 угроз на заблокированных адресах) – пять наиболее частых угроз с IP-адресов, заблокированных профилями Защиты DNS-трафика.

  - NGFW. DNS Security. Top-5 Threats for Redirected Addresses (Топ 5 угроз на перенаправленных адресах) – пять наиболее частых угроз с IP-адресов, перенаправленных профилями Защиты DNS-трафика.

  - NGFW. DNS Security. Top-5 Source IP Addresses With the Most Blocked Web Traffic (Топ 5 IP-адресов источника с наибольшим объемом заблокированного веб-трафика) – пять IP-адресов источника с наибольшим объемом трафика, заблокированного профилями Защиты DNS-трафика.

  - NGFW. DNS Security. Top-5 Redirected Hostnames (Топ 5 перенаправленных доменов) – пять доменов, наиболее часто перенаправляемых профилями Защиты DNS-трафика.

  - NGFW. DNS Security. Top-5 Destination IP Addresses With the Most Blocked Web Traffic (Топ 5 IP-адресов назначения с наибольшим объемом заблокированного веб-трафика) – пять IP-адресов назначения с наибольшим объемом трафика, заблокированного профилями Защиты DNS-трафика.

  - NGFW. DNS Security. Top-5 Source IP Addresses With the Most Redirected Web Traffic (Топ 5 IP-адресов источника с наибольшим объемом перенаправленного веб-трафика) – пять IP-адресов источника, наиболее часто перенаправляемых профилями Защиты DNS-трафика.

- Макет **NGFW Web Control & URL Web Antivirus**:

  - NGFW. URL Web Antivirus. Top-5 Web Categories for Blocked URLs (Топ 5 веб-категорий заблокированных URL) – пять наиболее частых веб-категорий URL, заблокированных профилями Веб-антивируса.

  - NGFW. URL Web Antivirus. Top-5 Destination IP Addresses With the Most Blocked Web Traffic (Топ 5 IP-адресов назначения с наибольшим объемом заблокированного веб-трафика) – пять IP-адресов с наибольшим объемом трафика, заблокированного профилями Веб-антивируса.

  - NGFW. Web Control. Top-5 Categories of Sites With the Most Warning Web Traffic (Топ 5 категорий веб-сайтов с предупреждением для веб-трафика) – пять категорий веб-сайтов, для которых наиболее часто было показано предупреждение от профилей Веб-Контроля.

  - NGFW. Web Control. Top-5 Categories of Sites With the Most Blocked Web Traffic (Топ 5 категорий веб-сайтов с заблокированным веб-трафиком) – пять категорий веб-сайтов с наибольшим объемом веб-трафика, заблокированного профилями Веб-Контроля.

  - NGFW. Web Control. Top-5 Destination IP Addresses With the Most Warning Web Traffic (Топ 5 IP-адресов назначения с предупреждением для веб-трафика) – пять IP-адресов назначения, для которых наиболее часто было показано предупреждение от профилей Веб-Контроля.

  - NGFW. Web Control. Top-5 Destination IP Addresses With the Most Blocked Web Traffic (Топ 5 IP-адресов назначения с заблокированным веб-трафиком) – пять IP-адресов назначения с наибольшим объемом веб-трафика, заблокированного Веб-Контроля.

- NGFW. Web Control. Top-5 Web Control Category Sources for Blocked Addresses (Топ 5 источников веб-категорий заблокированных адресов) – пять наиболее частых источников, от которых были получены веб-категории заблокированных URL.

- NGFW. Web Control. Top-5 Web Control Category Sources for Redirected Addresses (Топ 5 источников веб-категорий перенаправленных адресов) – пять наиболее частых источников, от которых были получены веб-категории перенаправленных URL.

- Макет **NGFW Firewall**:

  - NGFW. Top-5 Application Services by Sessions (Топ 5 прикладных сервисов по сессиям) – пять наиболее используемых прикладных сервисов по количеству сессий.

  - NGFW. Top-5 Application Services by Traffic, MB (Топ 5 прикладных сервисов по трафику, в МБ) – пять наиболее используемых прикладных сервисов по объему трафика, в МБ.

  - NGFW. Top-5 Application Protocols by Sessions (Топ 5 прикладных протоколов по количеству сессий) – пять наиболее используемых протоколов приложений по количеству сессий.

  - NGFW. Top-5 Application Protocols by Traffic, MB (Топ 5 прикладных протоколов по трафику, в МБ) – пять наиболее используемых протоколов приложений по объему трафика, в МБ.

  - NGFW. Top-5 Client Applications by Sessions (Топ 5 клиентских приложений по сессиям) – пять наиболее используемых клиентских приложений по количеству сессий.

  - NGFW. Top-5 Client Applications by Traffic, MB (Топ 5 клиентских приложений по трафику, в МБ) – пять наиболее используемых клиентских приложений по объему трафика, в МБ.

  - NGFW. Top-5 Source IP by Traffic, MB (Топ 5 IP-адресов источника по трафику, в МБ) – пять IP-адресов источника с наибольшим объемом трафика, в МБ.

  - NGFW. Top-5 Destination IP by Traffic, MB (Топ 5 IP-адресов назначения по трафику, в МБ) – пять IP-адресов назначения с наибольшим объемом трафика, в МБ.

  - NGFW. Top-5 Web Sites by Sessions (Топ 5 веб-сайтов по сессиям) – пять доменов с наибольшим количеством сессий.

  - NGFW. Top-5 Web Sites by Traffic, MB (Топ 5 доменов по трафику, в МБ) – пять доменов с наибольшим объемом трафика, в МБ.

По умолчанию для преднастроенных макетов указан период обновления **Никогда**. Вы можете изменять эти макеты при необходимости.

О режиме Просмотра только панели мониторинга

Вы можете настраивать режим Просмотра только панели мониторинга для сотрудников, которые не управляют сетью, но хотят просматривать статистику защиты сети в Open Single Management Platform (например, это может быть топ-менеджер). Когда у пользователя включен этот режим, у пользователя отображается только панель мониторинга с предопределенным набором виджетов. Таким образом, пользователь может просматривать указанную в виджетах статистику, например, состояние защиты всех управляемых устройств, количество недавно обнаруженных угроз или список наиболее частых угроз в сети.

При работе пользователя в режиме Просмотра только панели мониторинга применяются следующие ограничения:

- Главное меню не отображается, поэтому пользователь не может изменить параметры защиты сети.
- Пользователь не может выполнять действия с виджетами, например, добавлять или скрывать их. Поэтому нужно разместить в панели мониторинга все необходимые пользователю виджеты и настроить их, например, задать правило подсчета объектов или указать период.

Вы не можете назначить режим Просмотра только панели мониторинга себе. Если вы хотите работать в этом режиме, обратитесь к системному администратору, поставщику услуг (MSP) или пользователю с правами **Изменение списков управления доступом объектов** в функциональной области **Общие функции: Права пользователя**.

Настройка режима Просмотра только панели мониторинга

Перед началом настройки режима Просмотра только панели мониторинга убедитесь, что выполнены следующие предварительные требования:

- У вас есть право **Изменение списков управления доступом объектов** в функциональной области **Общие функции: Права пользователя**. Если у вас нет этого права, вкладка для настройки режима будет отсутствовать.
- Пользователь с правом **Чтение** в области **Общие функции: Базовая функциональность**.

> Если в вашей сети выстроена иерархия Серверов администрирования, для настройки режима Просмотра только панели мониторинга перейдите на тот Сервер, на котором учетная запись пользователя доступна на вкладке **Пользователи** в разделе **Пользователи и роли → Пользователи и группы**. Это может быть главный Сервер или физический подчиненный Сервер. На виртуальном Сервере администрирования настроить режим Просмотра только панели мониторинга невозможно.

Чтобы настроить режим Просмотра только панели мониторинга:

1. В главном окне приложения перейдите в раздел **Пользователи и роли → Пользователи и группы** и выберите вкладку **Пользователи**.
2. Нажмите на имя учетной записи пользователя, для которой вы хотите настроить панель инструментов с виджетами.
3. В открывшемся окне свойств учетной записи выберите вкладку **Панель мониторинга**.

   На открывшейся вкладке отображается та же панель мониторинга, что и для пользователя.
4. Если параметр **Отображать режим Просмотра только панели мониторинга** включен, выключите его переключателем.

   Когда этот параметр включен, также невозможно изменить панель мониторинга. После выключения параметра можно управлять виджетами.

5. Настройте внешний вид панели мониторинга. Набор виджетов, подготовленный на вкладке **Панель мониторинга**, доступен пользователю с настраиваемой учетной записью. Пользователь с такой учетной записью не может изменять какие-либо параметры или размер виджетов, добавлять или удалять виджеты с панели мониторинга. Поэтому настройте их под пользователя, чтобы он мог просматривать статистику защиты сети. Для этого на вкладке **Панель мониторинга** можно выполнять те же действия с виджетами, что и в разделе **Мониторинг → Панель мониторинга**:

   - Добавлять виджеты в панель мониторинга.
   - Скрывать виджеты, которые не нужны пользователю.
   - Перемещать виджеты в определенном порядке.
   - Изменять размер или внешний вид виджетов.
   - Изменять параметры виджетов.

6. Переключите переключатель, чтобы включить параметр **Отображать режим Просмотра только панели мониторинга**.

   После этого пользователю доступна только панель мониторинга. Пользователь может просматривать статистику, но не может изменять параметры защиты сети и внешний вид панели мониторинга. Так как вам отображается та же панель мониторинга, что и для пользователя, вы также не можете изменить панель мониторинга.

   Если оставить этот параметр выключенным, у пользователя отображается главное меню, поэтому он может выполнять различные действия в Open Single Management Platform, в том числе изменять параметры безопасности и виджеты.

7. Нажмите на кнопку **Сохранить**, когда закончите настройку режима Просмотра только панели мониторинга. Только после этого подготовленная панель мониторинга будет отображаться у пользователя.

8. Если пользователь хочет просмотреть статистику поддерживаемых приложений "Лаборатории Касперского" и ему нужны для этого права доступа, настройте права для этого пользователя. После этого данные приложений "Лаборатории Касперского" отображаются у пользователя в виджетах этих приложений.

Теперь пользователь может входить в Open Single Management Platform под настраиваемой учетной записью и просматривать статистику защиты сети в режиме Просмотра только панели мониторинга.

Просмотр и сохранение ревизии политики

Ревизия политики — это сохраненное состояние политики, которое автоматически фиксируется каждый раз при ее изменении и сохранении. Ревизия сдержит параметры политики, профили и правила их активации, метаданные о дате, а также пользователе и IP-адресе, которые создали эту ревизию. Open Single Management Platform позволяет просматривать ревизию политики, чтобы отслеживать изменения настроек, а также сохранять ревизию в файл JSON.

Просмотр и сохранение ревизии политики доступны, если соответствующий веб-плагин управления поддерживает эту функцию.
Опции доступны для политик Сервера администрирования, Агента администрирования, Kaspersky Endpoint Security for Windows (начиная с версии веб-плагина 14.0), Kaspersky Endpoint Security for Linux (начиная с версии веб-плагина 12.4) и Kaspersky Endpoint Security for Mac (начиная с версии веб-плагина 12.2.1 Patch A).

Чтобы просмотреть ревизию политики:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на ревизию политики, которую вы хотите просмотреть и перейдите в раздел **История ревизий**.
3. В списке ревизий политики нажмите на номер ревизии, которую вы хотите просмотреть.

   В открывшемся отчете доступна информация о параметрах политики, ее профилях и правилах активации для них.

   Если размер ревизии превышает 10 МБ, просмотреть ее с помощью OSMP Console невозможно. Вам будет предложено сохранить выбранную ревизию в файл JSON.

   Если размер ревизии не превышает 10 МБ, отображается отчет в формате HTML с параметрами выбранной ревизии политики. Так как отчет отображается во всплывающем окне, убедитесь, что в вашем браузере разрешены всплывающие окна.

В случае политик Kaspersky Endpoint Security for Windows и Kaspersky Endpoint Security for Mac в отчете не будет информации о профилях политик.

Чтобы сохранить ревизию политики в файл JSON,

В списке ревизий политики выберите ревизию, которую вы хотите сохранить и нажмите на кнопку **Сохранить в файл**.

Ревизия сохранена в файле JSON.

При необходимости вы можете сравнить ревизии политики.

Сравнение ревизий политики

Вы можете сравнить предыдущие ревизии политики с ее текущей ревизией, сравнить различные ревизии, выбранные в списке, или сравнить ревизию одной политики с ревизией другой политики. Параметры доступны для политик Сервера администрирования, Агента администрирования, Kaspersky Endpoint Security for Windows (начиная с версии веб-плагина 14.0) и Kaspersky Endpoint Security for Mac (начиная с версии веб-плагина 12.2.1 Patch A).

Сравнение ревизий политик доступно, если соответствующие веб-плагины управления поддерживает эту функцию.

Чтобы просмотреть ревизию политики:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на политику, ревизии которой вы хотите сравнить.

   Откроется окно свойств политики.
3. Перейдите на вкладку **История ревизий** и установите флажки рядом с ревизиями, которые нужно сравнить.

4. В панели инструментов нажмите на кнопку **Сравнить** и в раскрывающемся списке выберите один из следующих вариантов:

   - **С текущей ревизией**, если вы хотите сравнить ревизию, выбранную на шаге 3, с последней сохраненной ревизией той же политики.
   - **Выбранные ревизии**, если вы хотите сравнить две ревизии, около которых вы установили флажки на шаге 3.

     Порядок установки флажков не влияет на результаты сравнения. По умолчанию более ранняя выбранная ревизия сравнивается с последней ревизией. Например, если вы установите флажки рядом с ревизиями 5 и 1, ревизия 1 будет сравниваться с ревизией 5. Отчет будет содержать информацию о параметрах ревизии 1, которые были добавлены, удалены или изменены по сравнению с ревизией 5.

   - **С ревизией другой политики**, если вы хотите сравнить ревизии двух разных политик.

     В открывшейся панели выполните следующие действия:

     a. В поле **Название приложения** выберите политику ревизии которой вы хотите сравнить: Агент администрирования или Сервер администрирования.

     b. В поле **Название политики** укажите название политики, ревизию которой вы хотите сравнить с той, которую вы выбрали на шаге 3.

     Отобразится список ревизий политики.

     c. Выберите нужную ревизию и нажмите на кнопку **Сравнить**.

Отчет сравнения ревизий отобразится в формате HTML на новой вкладке вашего браузера.

Если результат сравнения превышает 10 МБ, отобразится соответствующее диалоговое окно. Вы можете нажать на кнопку **Сохранить в файл**, чтобы сохранить отчет в виде файла, или отменить операцию.

Отчет отображается на языке интерфейса вашей OSMP Console. Вы можете развернуть некоторые разделы отчета, нажав на значок стрелки вниз (▼) рядом с разделом или свернуть раздел, нажав на значок стрелки вверх (▲).

Отчет содержит следующую информацию:

- Логотип "Лаборатория Касперского".
- Название отчета.
- Время и дата создания отчета.
- Имя политики, Сервер администрирования и группа администрирования, в которую входит политика (политики), ревизии которой сравнивались.
- Кнопка **Сохранить как HTML**. Если вы нажмете на кнопку, отчет будет сохранен на вашем устройстве.

- Раздел **Сводная информация**, в котором отображается общая информация о сравниваемых ревизиях: имя политики (политик), номер ревизии, время и дата, когда ревизия была сохранена, пользователь, который сохранил ревизию, и описание ревизии.

  Для унаследованных политик пользователь не отображается.

- Различия сравниваемых ревизий. Различия отображаются в следующих разделах:

  - **Добавленные параметры.**
  - **Удаленные параметры.**
  - **Измененные параметры.**
  - **Параметры доступны только для объекта 1** (если вы сравнивали ревизии двух разных политик).
  - **Параметры доступны только для объекта 2** (если вы сравнивали ревизии двух разных политик).

  Раздел не отображается, если в нем нет данных.

Откат изменений объекта к предыдущей ревизии

В случае необходимости вы можете откатить изменения объекта. Например, вам может понадобиться вернуть параметры политики к состоянию на определенную дату.

Чтобы откатить изменения объекта:

1. В окне свойств объекта перейдите на вкладку **История ревизий**.
2. В списке ревизий объекта выберите ревизию, к которой нужно откатить изменения.
3. Нажмите на кнопку **Откатить**.
4. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

   Произойдет откат к выбранной ревизии. В списке ревизий объекта отобразится запись о выполненном действии. В описании ревизии отобразится информация о номере ревизии, к которой вы вернули объект.

Операция отката доступна только для политик и задач.

Отслеживание состояния сервисов

Решение Kaspersky SIEM Cloud построено на микросервисной архитектуре. Каждый компонент решения, например коллекторы, корреляторы или хранилища, работает как отдельный сервис. Поэтому общее "здоровье" работы решения складывается из состояния работы всех его сервисов. Ряд средств для отслеживания состояния работы сервисов работает "из коробки" и не требует дополнительной настройки. При этом вы можете настроить некоторые параметры для отслеживания состояния сервисов по своему усмотрению. Это поможет точечно отслеживать проблемы в работе сервисов, характерные для конкретной конфигурации решения или инфраструктуры организации.

Встроенные механизмы диагностики работы сервисов

Одним из способов определить текущее состояние сервиса является статус. Статус сервиса определяется автоматически на основании следующей информации:

- доступность сервиса;
- наличие ошибок в файлах журнала сервиса;
- значения настраиваемых параметров.

Возможные статусы сервисов

- Зеленый – сервис работает и доступен с сервера Ядра Kaspersky SIEM Cloud.
- Красный – сервис не работает или не доступен с сервера Ядра Kaspersky SIEM Cloud.
- Желтый – сервис работает, но в журнале сервиса есть ошибки или для сервиса есть алерты от Victoria Metrics. Сообщение об ошибке отображается, если навести курсор мыши на статус сервиса. Желтый статус применяется ко всем сервисам, кроме агента.
- Фиолетовый – изменился конфигурационный файл сервиса, но другие ошибки отсутствуют. Если у сервиса некорректный конфигурационный файл и есть ошибки, например от Victoria Metrics, статус сервиса будет желтым.
- Серый – в удаленном тенанте был работающий сервис, который продолжает работать. Сервисы в сером статусе остаются после удаления тенанта, чтобы вы могли скопировать идентификатор и удалить сервисы на серверах. Удалить сервисы с серым статусом может только Главный администратор. При удалении тенанта сервисы этого тенанта привязываются к тенанту Main.

При смене статуса сервиса создается событие аудита. К событиям аудита можно создавать поисковые запросы, создавать по таким событиям виджеты или использовать их в правилах корреляции.

Еще одним инструментом для отслеживания работы сервисов являются метрики Kaspersky SIEM Cloud, которые представляют собой панели мониторинга с информацией о метриках и визуализацией ключевых параметров работы различных сервисов Kaspersky SIEM Cloud. Этот инструмент позволяет отслеживать состояние всех сервисов, кроме холодного хранилища и агента. Например, с помощью метрик можно выявить нехватку выделенных ресурсов.

Для доступа к метрикам Kaspersky SIEM Cloud у пользователя должна быть соответствующая роль или права доступа.

Настройка параметров для отслеживания состояния сервисов

Пороговые значения параметров для мониторинга сервисов Kaspersky SIEM Cloud могут настраивать только пользователи с ролью Главный администратор.

Чтобы настроить параметры сервисов:

1. В веб-интерфейсе откройте раздел **Параметры** → **Другое** → **Мониторинг сервисов**.
2. Укажите значения параметров мониторинга для сервисов.

   Мониторинг сервисов не распространяется на холодное хранилище.

   Если вы указали значение, которое не подходит по диапазону или формату, значение будет сброшено до установленного ранее.
3. Нажмите **Сохранить**.

Kaspersky SIEM Cloud зарегистрирует событие аудита Пороговые значения для мониторинга сервисов изменены.

Kaspersky SIEM Cloud отслеживает состояние сервисов по заданным параметрам. Если заданные пороговые значения будут превышены, произойдут следующие изменения:

- Kaspersky SIEM Cloud зарегистрирует событие аудита Зарегистрирован алерт Metrics для сервиса.
- Kaspersky SIEM Cloud отправит уведомление Главному администратору по электронной почте.
- Сервисы отобразятся в разделе **Активные сервисы** в желтом статусе. Если вы наведете курсор на значок статуса, отобразится сообщение об ошибке.

  Чтобы найти сервисы с ошибками, в разделе **Активные сервисы** вы можете отфильтровать сервисы по статусам или указать в поле поиска слово из текста ошибки, например `QPS` или `buffer`, и нажать **ENTER**. Использовать специальные символы `"`, `}`, `{` невозможно.

Примеры отслеживания состояния сервисов

В следующих примерах показано, каким образом вы можете отслеживать состояние сервисов.

1. Если в разделе **Активные сервисы** сервис коллектора находится в желтом статусе и вы видите сообщение **Enrichment errors increasing**, вы можете выполнить следующие действия:

   - Перейти в раздел **Метрики** → **<тип сервиса>** → **<имя сервиса>** → **Enrichment** → **Errors** и выяснить, какое именно обогащение работает с ошибками, а также просмотреть график, чтобы уточнить когда именно началась проблема и отследить динамику.

   - Проверить параметры подключения DNS или Kaspersky CyberTrace, поскольку вероятной причиной ошибок обогащения может быть недоступность DNS-сервера или ошибки обогащения Kaspersky CyberTrace.

2. Если в разделе **Активные сервисы** сервис коллектора находится в желтом статусе и вы видите сообщение **Output Event Loss increasing**, вы можете выполнить следующие действия:

   - Перейти в раздел **Метрики** → **<тип сервиса>** → **<имя сервиса>** → **IO** → **Output Event Loss** и просмотреть график, чтобы уточнить когда именно началась проблема и отследить динамику.

   - Проверить доступность и правильность подключения точки назначения или выяснить, почему превышен размер буфера, поскольку вероятной причиной потери событий может быть недоступность точки назначения или превышение размера буфера.

Использование правил корреляции

Для отслеживания состояния сервисов Kaspersky SIEM Cloud вы можете использовать правила корреляции. Для этого вы можете скачать из репозитория пакет правил корреляции [OOTB] KUMA package - RU или [OOTB] KUMA package - ENG, в который также входят правила корреляции для мониторинга работоспособности сервисов Kaspersky SIEM Cloud. Например, из этого пакета вы можете использовать правило `R503_11_Оповещение о возможной проблеме с производительностью служб KUMA`, привязав его к коррелятору. В результате работы этого правила корреляции Kaspersky SIEM Cloud будет создавать алерт при создании события аудита Зарегистрирован алерт Metrics для сервиса.

Создание виджетов и отчетов

Для визуализации состояния сервисов Kaspersky SIEM Cloud вы можете добавить в панель мониторинга виджеты, настроенные на отображение статистики по событиям аудита Зарегистрирован алерт Metrics для сервиса или Статус сервиса изменен.

Выключение мониторинга сервисов

Чтобы выключить мониторинг сервисов:

1. В веб-консоли Kaspersky SIEM Cloud перейдите в раздел **Параметры** → **Другое** → **Мониторинг сервисов**.

2. Если вы хотите выключить мониторинг сервисов только для коллекторов, в блоке параметров **Коллекторы** установите флажок **Отключить ошибки коннекторов**.

   Будет отключен только анализ метрики **Connector errors** для коллекторов.

3. Если вы хотите выключить мониторинг всех сервисов, установите переключатель **Состояние** в положение выключено.

Мониторинг сервисов Kaspersky SIEM Cloud будет выключен, при этом сервисам не будет присваиваться желтый статус.

Просмотр метрик Kaspersky SIEM Cloud

Для отслеживания работы своих компонентов, потока событий, контекста корреляции в Kaspersky SIEM Cloud выполняется сбор и хранение большого количества параметров. Для сбора, хранения и анализа параметров используется решение VictoriaMetrics, представляющее собой СУБД в формате временных рядов. Полученные метрики можно просматривать с помощью Grafana. В разделе **Мониторинг** → **Метрики** представлены панели мониторинга с визуализацией ключевых параметров работы различных компонентов Kaspersky SIEM Cloud.
Сервис Ядра Kaspersky SIEM Cloud выполняет настройку параметров VictoriaMetrics и Grafana автоматически, участие пользователя не требуется.

Также метрики Kaspersky SIEM Cloud можно просмотреть в разделе **Панель мониторинга**:

1. В главном меню перейдите в раздел **Мониторинг** → **Панель мониторинга** и выберите вкладку **Обнаружение и реагирование**.

2. Нажмите на значок с многоточием (⋮).

3. Нажмите на кнопку **Перейти к метрикам Kaspersky SIEM Cloud**.

Полученные метрики можно просматривать с помощью решения Grafana. RPM-пакет службы kuma-core генерирует конфигурацию Grafana и создает отдельную панель мониторинга для визуализации показателей каждой службы. Графики в разделе **Метрики** появляются с задержкой примерно в 1,5 минуты.

Полную информацию о метриках вы можете найти в Консоли OSMP в разделе **Показатели**. При выборе этого раздела открывается автоматически обновляемый портал Grafana, развернутый во время установки Ядра KUMA. Если в разделе **Метрики** вы видите core: <номер порта>, это означает, что Kaspersky SIEM Cloud развернута в отказоустойчивой конфигурации и метрики получены с устройства, на котором было **установлено Ядро**. В прочих конфигурациях отображается имя устройства, с которого Kaspersky SIEM Cloud получает метрики.

Чтобы определить, на каком хосте работает Ядро, в терминале одного из контроллеров выполните следующую команду:

```
k0s kubectl get pod -n kuma -o wide
```

Метрики коллектора

Название метрики	Описание
IO (ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.	
Processing EPS	Количество событий, обработанных за секунду.
Output EPS	Количество событий, отправленных точке назначения за секунду.
Output Latency	Время в миллисекундах, затраченное на отправку пакета событий точке назначения и получение от нее ответа. Отображается медиана.
Output Errors	Количество ошибок, возникших за секунду при отправке пакетов событий точке назначения. Сетевые ошибки и ошибки записи в дисковый буфер точки назначения отображаются отдельно.
Output Event Loss	Количество событий, потерянных за секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер точки назначения. События также теряются, если точка назначения отвечает кодом ошибки, например при недействительном запросе.
Output Disk Buffer Size	Размер дискового буфера коллектора, связанного с точкой назначения, в байтах. Если отображается ноль, в дисковой буфер коллектора не помещен ни один пакет событий, и сервис работает правильно.
Write Network BPS	Количество байт, принятых в сеть за секунду.
Connector errors	Количество ошибок в журналах событий коннектора.

Normalization (Нормализация) – показатели, относящиеся к нормализаторам.	
Raw & Normalized event size	Размер сырого события и размер нормализованного события. Отображается среднее значение.
Errors	Количество ошибок нормализации в секунду.

Filtration – показатели, относящиеся к фильтрам.	
EPS	Количество событий, удовлетворяющих условиям фильтра и отправленных в обработку в секунду. Коллектор обрабатывает события, удовлетворяющие условиям фильтра, только если пользователь добавил фильтр в конфигурацию службы коллектора.

Aggregation (Агрегация) – показатели, относящиеся к правилам агрегации.	
EPS	Количество событий, полученных и созданных правилом агрегации в секунду. Этот показатель помогает определить эффективность правил агрегации.
Buckets	Количество контейнеров в правиле агрегации.

Enrichment – показатели, относящиеся к правилам обогащения.	
Cache RPS	Количество запросов к локальному кешу в секунду.
Source RPS	Количество запросов в секунду, отправленных источнику обогащения, например словарю.
Source Latency	Время в миллисекундах, прошедшее после отправки запроса источнику обогащения и после получения от него ответа. Отображается среднее значение.
Queue	Размер очереди запросов на обогащение. Эта метрика помогает найти "узкие места" в правилах обогащения.
Errors	Количество ошибок в секунду при отправке запросов к источнику обогащения.

Показатели коррелляторов

Название метрики	Описание
IO (ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.	
Processing EPS	Количество событий, обработанных за секунду.
Output EPS	Количество событий, отправленных точке назначения за секунду.
Output Latency	Время в миллисекундах, затраченное на отправку пакета событий точке назначения и получение от нее ответа. Отображается медиана.
Output Errors	Количество ошибок, возникших за секунду при отправке пакетов событий точке назначения. Сетевые ошибки и ошибки записи в дисковый буфер точки назначения отображаются отдельно.
Output Event Loss	Количество событий, потерянных за секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер точки назначения. События также теряются, если точка назначения отвечает кодом ошибки, например при недействительном запросе.
Output Disk Buffer Size	Размер дискового буфера коллектора, связанного с точкой назначения, в байтах. Если отображается ноль, в дисковой буфер коллектора не помещен ни один пакет событий, и сервис работает правильно.

Correlation – показатели, относящиеся к правилам корреляции.	
EPS	Количество событий корреляции в секунду, созданных правилом корреляции.
Buckets	Количество контейнеров в правиле корреляции стандартного типа.
Rate Limiter Hits	Количество превышений правилом корреляции предельного значения срабатываний в секунду.
Active Lists OPS	Количество запросов на выполнение операций, отправленных активному листу в секунду, и сами операции.
Active Lists Records	Количество записей в активном листе.
Active Lists On-Disk Size	Размер активного листа на диске в байтах.

Enrichment – показатели, относящиеся к правилам обогащения.	
Cache RPS	Количество запросов к локальному кешу в секунду.
Source RPS	Количество запросов в секунду, отправленных источнику обогащения, например словарю.

Source Latency	Время в миллисекундах, прошедшее после отправки запроса источнику обогащения и после получения от него ответа. Отображается среднее значение.
Queue	Размер очереди запросов на обогащение. Эта метрика помогает найти "узкие места" в правилах обогащения.
Errors	Количество ошибок в секунду при отправке запросов к источнику обогащения.

Response – показатели, связанные с правилами реагирования.	
RPS	Количество срабатываний правила реагирования в секунду.

Метрики хранилища

Название метрики	Описание
ClickHouse/General – показатели, относящиеся к общим параметрам кластера ClickHouse.	
Active Queries	Количество активных запросов, отправленных кластеру ClickHouse. Эта метрика отображается для каждого экземпляра ClickHouse.
QPS	Количество запросов в секунду, отправленных кластеру ClickHouse.
Failed QPS	Количество неудачных запросов в секунду, отправленных кластеру ClickHouse.
Allocated memory	Объем оперативной памяти в гигабайтах, выделенной процессу ClickHouse.

ClickHouse/Insert – метрики, относящиеся к вставке событий в экземпляр ClickHouse.	
Insert EPS	Количество событий в секунду, вставленных в экземпляр ClickHouse.
Insert QPS	Количество запросов в секунду на вставку событий в экземпляр ClickHouse, отправленных кластеру ClickHouse. Если на метрике **Insert QPS** растет очередь из запросов и показатель превышает 1, рекомендуется посмотреть также значение метрики **Batch size**, чтобы скорректировать параметры буферизации хранилища в параметрах конфигурации службы хранилища. Пример: Показатель метрики **Insert QPS** превышает 1 и равен 8. Показатель **Batch size** – 1,2 ГБ (в байтах). В этом случае следует определить размер буфера, перемножив показатели метрик **Insert QPS** и **Batch size**: 8 * 1.2 = 9.6 ГБ. Полученное значение 9.6 следует округлить и указать в байтах (например, 10000000000 байт) в качестве значения параметра **Размер буфера** на вкладке **Дополнительные параметры** в настройках конфигурации сервиса хранилища. Также следует указать значение параметра **Интервал очистки буфера** – 2 с. Увеличение размера буфера и интервала очистки буфера позволит разгрузить очередь запросов. При нормальных условиях показатель метрики **Insert QPS** не превышает 1.
Failed Insert QPS	Количество неудачных запросов в секунду на вставку событий в экземпляр ClickHouse, отправленных кластеру ClickHouse.
Delayed Insert QPS	Количество отложенных запросов в секунду на вставку событий в экземпляр ClickHouse, отправленных кластеру ClickHouse. Запросы были отложены узлом ClickHouse из-за превышения мягкого ограничения активного объединения запросов.
Rejected Insert QPS	Количество отклоненных запросов в секунду на вставку событий в экземпляр ClickHouse, отправленных кластеру ClickHouse. Запросы были отложены узлом ClickHouse из-за превышения жесткого ограничения активного объединения запросов.

Active Merges	Количество активных объединений запросов.
Distribution Queue	Количество временных файлов с событиями, которые не удалось вставить в экземпляр ClickHouse из-за его недоступности. Эти события не могут быть найдены с помощью поиска.

ClickHouse/Select – показатели, относящиеся к выборкам событий в экземпляре ClickHouse.	
Select QPS	Количество запросов на выборку событий в секунду в экземпляре ClickHouse, отправленных кластеру ClickHouse.
Failed Select QPS	Количество неудачных запросов на выборку событий в секунду в экземпляре ClickHouse, отправленных кластеру ClickHouse.

ClickHouse/Replication – метрики, относящиеся к репликам узлов ClickHouse.	
Active Zookeeper Connections	Количество активных подключений к узлам кластера Zookeeper. При нормальной работе это количество должно быть равно количеству узлов в кластере Zookeeper.
Read-only Replicas	Количество реплик узлов ClickHouse, доступных только для чтения. При нормальной работе таких реплик узлов ClickHouse нет.
Active Replication Fetches	Количество активных процессов скачивания данных с узла ClickHouse при репликации данных.
Active Replication Sends	Количество активных процессов отправки данных узлу ClickHouse при репликации данных.
Active Replication Consistency Checks	Количество активных проверок согласованности данных на репликах узлов ClickHouse при репликации данных.

ClickHouse/Networking – показатели, относящиеся к сети кластера ClickHouse.	
Active HTTP Connections	Количество активных подключений к HTTP-серверу кластера ClickHouse.
Active TCP Connections	Количество активных подключений к TCP-серверу кластера ClickHouse.
Active Interserver Connections	Количество активных межсервисных соединений между узлами ClickHouse.

Показатели Ядра KUMA

Название метрики	Описание
Raft – метрики, связанные с чтением и обновлением состояния Ядра KUMA.	
Lookup RPS	Количество запросов процедуры поиска в секунду, отправленных в Ядро KUMA, и сами процедуры.
Lookup Latency	Время в миллисекундах, затраченное на выполнение процедур поиска и на выполнение самих процедур. Отображается время для 99-го процентиля процедур поиска. Один процент процедур поиска может занять больше времени.
Propose RPS	Количество запросов на выполнение процедур обновления состояния Raft (SQLite), отправленных Ядру в секунду, и сами процедуры.
Propose Latency	Время в миллисекундах, затраченное на выполнение процедур обновления состояния Raft (SQLite), и сами процедуры. Отображается время для 99-го процентиля процедур обновления состояния. Один процент процедур обновления состояния может занять больше времени.

Название метрики	Описание
Data mining – метрики, относящиеся к сбору и анализу данных	
Executing Rules	Количество запущенных планировщиков для выполнения запросов сбора и анализа данных.
Queued Rules	Количество планировщиков для выполнения запросов сбора и анализа данных в очереди.
Execution Errors	Количество ошибок при выполнении запуска планировщика сбора и анализа данных.
Execution Latency	Время выполнения запросов планировщика.
Tasks – метрики, относящиеся к мониторингу выполнения задач на Ядре Kaspersky SIEM Cloud	
Active tasks	Количество выполняемых задач за единицу времени.
Task Execution latency	Время выполняемых задач в секундах.
Errors	Количество ошибок при выполнении задач.

API – метрики, относящиеся к запросам API.	
RPS	Количество запросов API к Ядру KUMA в секунду.
Latency	Время в миллисекундах, затраченное на обработку одного запроса API к Ядру KUMA. Отображается среднее значение.
Errors	Количество ошибок в секунду при отправке API-запросов к Ядру KUMA.

Notification Feed – показатели, относящиеся к активности пользователей.	
Subscriptions	Количество клиентов, подключенных к Ядру KUMA через SSE для получения сообщений сервера в реальном времени. Это число обычно равно количеству клиентов, использующих Консоль Kaspersky SIEM Cloud.
Errors	Количество ошибок в секунду при отправке уведомлений пользователям.

Schedulers – показатели, относящиеся к задачам Ядра KUMA.	
Активная	Количество повторяющихся активных системных задач. Задачи, созданные пользователем, игнорируются.
Latency	Время в миллисекундах, затраченное на выполнение задачи. Отображается среднее значение.
Errors	Количество ошибок в секунду, возникших при выполнении задач.

Метрики агента Kaspersky SIEM Cloud

Название метрики	Описание
IO (ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.	
Processing EPS	Количество событий, обработанных за секунду.
Output EPS	Количество событий, отправленных точке назначения за секунду.
Output Latency	Время в миллисекундах, затраченное на отправку пакета событий точке назначения и получение от нее ответа. Отображается медиана.
Output Errors	Количество ошибок, возникших за секунду при отправке пакетов событий точке назначения. Сетевые ошибки и ошибки записи в дисковый буфер точки назначения отображаются отдельно.
Output Event Loss	Количество событий, потерянных за секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер точки назначения. События также теряются, если точка назначения отвечает кодом ошибки, например при недействительном запросе.
Output Disk Buffer Size	Размер дискового буфера коллектора, связанного с точкой назначения, в байтах. Если отображается ноль, в дисковой буфер коллектора не помещен ни один пакет событий, и сервис работает правильно.
Write Network BPS	Количество байт, принятых в сеть за секунду.

Метрики маршрутизаторов событий

Название метрики	Описание
IO (ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.	
Processing EPS	Количество событий, обработанных за секунду.
Output EPS	Количество событий, отправленных точке назначения за секунду.
Output Latency	Время в миллисекундах, затраченное на отправку пакета событий точке назначения и получение от нее ответа. Отображается медиана.
Output Errors	Количество ошибок, возникших за секунду при отправке пакетов событий точке назначения. Сетевые ошибки и ошибки записи в дисковый буфер точки назначения отображаются отдельно.
Output Event Loss	Количество событий, потерянных за секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер точки назначения. События также теряются, если точка назначения отвечает кодом ошибки, например при недействительном запросе.
Output Disk Buffer Size	Размер дискового буфера коллектора, связанного с точкой назначения, в байтах. Если отображается ноль, в дисковой буфер коллектора не помещен ни один пакет событий, и сервис работает правильно.
Write Network BPS	Количество байт, принятых в сеть за секунду.
Connector Errors	Количество ошибок в журнале коннектора.

Метрики, общие для всех сервисов

Название метрики	Описание
Process – общие метрики процесса.	
Memory	Использование оперативной памяти (RSS) в мегабайтах.

Название метрики	Описание
DISK BPS	Количество байтов, считываемых с диска или записываемых на диск в секунду.
Network BPS	Количество байтов, получаемых/передаваемых в сеть в секунду.
Network Packet Loss	Количество сетевых пакетов, потерянных в секунду.
GC Latency	Время в миллисекундах, затраченное на выполнение цикла сборщика мусора GO (Garbage Collector). Отображается среднее значение.
Goroutines	Количество активных горутин. Это число отличается от количества потоков операционной системы.

OS – показатели, относящиеся к операционной системе.	
Load	Средняя нагрузка.
Процессор	Загрузка процессора в процентах.
Memory	Использование оперативной памяти (RSS) в процентах.
Disk	Использование дискового пространства в процентах.

Срок хранения метрик

По умолчанию данные о работе Kaspersky SIEM Cloud хранятся 3 месяца. Этот срок можно изменить.

Чтобы изменить срок хранения метрик Kaspersky SIEM Cloud:

1. Войдите в ОС сервера, на котором установлено Ядро Kaspersky SIEM Cloud.
2. В файле /etc/systemd/system/multi-user.target.wants/kuma-victoria-metrics.service в параметре ExecStart измените флаг `--retentionPeriod=<срок хранения метрик в месяцах>`, подставив нужный срок. Например, `--retentionPeriod=4` означает, что метрики будут храниться 4 месяца.
3. Перезапустите Kaspersky SIEM Cloud, выполнив последовательно следующие команды:
   a. `systemctl daemon-reload`
   b. `systemctl restart kuma-victoria-metrics`

Срок хранения метрик изменен.

Условия срабатывания алертов по метрикам Kaspersky SIEM Cloud

Если значение метрики Kaspersky SIEM Cloud о работе сервиса превышает пороговое значение соответствующего параметра, настроенного в разделе **Мониторинг сервисов**, от решения VictoriaMetrics поступает алерт и в статусе этого сервиса отображается сообщение об ошибке.

Получение алертов от VictoriaMetrics происходит со следующей периодичностью:

- VictoriaMetrics собирает информацию от сервисов Kaspersky SIEM Cloud каждые 15 секунд.
- VictoriaMetrics обновляет алерты для сервисов Kaspersky SIEM Cloud каждую минуту.
- Сервис Ядра Kaspersky SIEM Cloud собирает информацию от VictoriaMetrics каждые 15 секунд.

Таким образом, общая длительность задержки в обновлении статуса сервиса может достигать не более 2-3 минут.

Если вы выключили получение алертов от VictoriaMetrics, некоторые сервисы Kaspersky SIEM Cloud все равно могут отображаться с желтым статусом. Это может произойти в следующих случаях:

- Для сервиса хранилище:
  - если алерт пришел по API запросу в параметре /status от ClickHouse;
  - если холодное хранилище сервиса Хранилище не проверяется.
- Для сервиса коллектор: если алерт пришел по API-запросу в параметре /status.
- Для сервиса коррелятор: если есть правило реагирования, для которого требуется модуль Advanced Responses, но этот модуль отсутствует в действующей лицензии или срок действия лицензии, в которой есть этот модуль, истек.

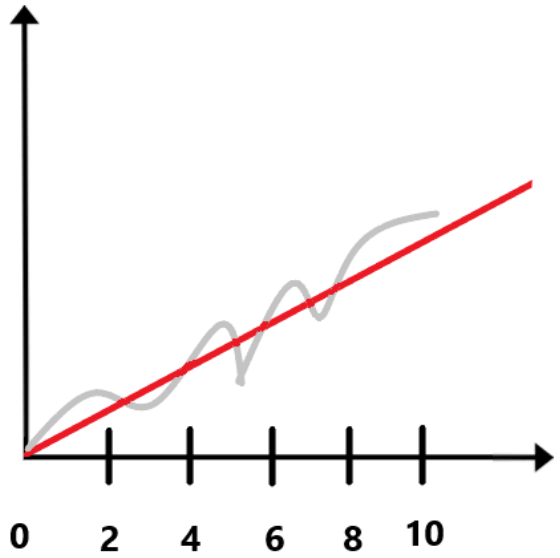
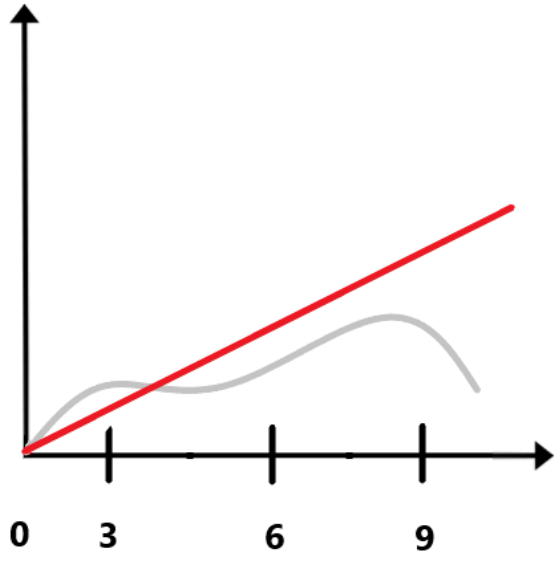
В таблице ниже представлена информация о том, какие сообщения об ошибке могут появиться в статусе сервиса при получении алерта от VictoriaMetrics и как и на основании каких метрик и параметров они рассчитываются. Подробнее о метриках Kaspersky SIEM Cloud, на основании которых могут сработать алерты VictoriaMetrics, см. Просмотр метрик Kaspersky SIEM Cloud.

Например, если в таблице **Активные сервисы** для сервиса отображается желтый статус и сообщение об ошибке `High distribution queue` (в таблице ниже – столбец "Сообщение об ошибке"), вы можете посмотреть данные в виджете **Enrichment**, метрика **Distribution Queue** (в таблице ниже – столбец "Метрики Kaspersky SIEM Cloud").

Описание сообщений об ошибках для сервисов Kaspersky SIEM Cloud

Сообщение об ошибке	Настраиваемые параметры для алертов	Метрика Kaspersky SIEM Cloud	Описание
`QPS threshold reached`	**Интервал/Окно QPS, минуты** **Порог QPS**	Clickhouse / General (общие параметры) → Failed QPS (безуспешные запросы в секунду)	Сообщение об ошибке отображается, если значение метрики Failed QPS превышает заданное значение параметра **Порог QPS** в течение интервала времени, заданного параметром **Интервал/Окно QPS, минуты**. Например, если из 100 запросов от решения VictoriaMetrics к сервису 25 пришли безуспешные, а параметр **Порог QPS** равен 0.2, алерт рассчитывается следующим образом: (25 / 100) * 100 > 0.2 * 100 25% > 20% Так как процент безуспешных запросов больше, чем заданный порог, для сервиса отобразится сообщение об ошибке.

Сообщение об ошибке	Настраиваемые параметры для алертов	Метрика Kaspersky SIEM Cloud	Описание
`Failed Insert QPS threshold reached`	**Интервал/Окно расчета ошибочных вставок QPS, минуты** **Порог вставок QPS**	Clickhouse / Insert (вставка) → Failed Insert QPS (безуспешные запросы на вставку в секунду)	Сообщение об ошибке отображается, если значение метрики Failed Insert QPS превышает заданное значение параметра **Порог вставок QPS** в течение интервала времени, заданного параметром **Интервал/Окно расчета ошибочных вставок QPS, минуты**. Например, если из 100 запросов от решения VictoriaMetrics к сервису 25 пришли безуспешные, а параметр **Порог вставок QPS** равен 0.2, алерт рассчитывается следующим образом: (25 / 100) * 100 > 0.2 * 100 25% > 20% Так как процент безуспешных запросов больше, чем заданный порог, для сервиса отобразится сообщение об ошибке.
`High distribution queue`	**Порог очереди распределения** **Интервал/Окно расчета очереди распределения, минуты**	Clickhouse / Insert (вставка) → Distribution Queue (очередь распределения)	Сообщение об ошибке отображается, если значение метрики Distribution Queue превышает заданное значение параметра **Порог очереди распределения** в течение интервала времени, заданного параметром **Интервал/Окно расчета очереди распределения, минуты**.
`Low disk space`	**Порог свободного места на диске**	OS (ОС) → Disk (диск)	Сообщение об ошибке отображается, если размер свободного места на диске (в процентах) в значении метрики Disk меньше, чем задано в параметре **Порог свободного места на диске**. Например, сообщение об ошибке отобразится, если раздел, на котором установлена Kaspersky SIEM Cloud, занимает все место на диске.
`Low disk partition space`	**Порог свободного места на разделе диска**	OS (ОС) → Disk (диск)	Сообщение об ошибке отображается, если размер свободного места в разделе диска, с которым работает Kaspersky SIEM Cloud (в процентах), осталось меньше, чем задано в параметре **Порог свободного места на разделе диска**. Например, сообщение об ошибке отобразится в следующих случаях: • При установке Kaspersky SIEM Cloud в отказоустойчивой конфигурации, когда диск подключается как том. • Если диск монтирован в раздел /opt.
`Output Event Loss increasing`	**Потери исходящих событий**	IO (ввод-вывод) → Output Event Loss (потеря событий)	Сообщение об ошибке отображается, если значение метрики Output Event Loss возрастает в течение одной минуты. Вы можете включить или выключить отображение этого сообщения об ошибке с помощью параметра **Потери исходящих событий**.

Сообщение об ошибке	Настраиваемые параметры для алертов	Метрика Kaspersky SIEM Cloud	Описание
`Disk buffer size increasing`	**Интервал/Окно увеличения дискового буфера, минуты**	IO (ввод-вывод) → Output Disk Buffer Size (размер дискового буфера)	Сообщение об ошибке отображается, если в течение 10 минут с интервалом, заданным параметром **Интервал/Окно увеличения дискового буфера, минуты**, значение метрики Output Disk Buffer Size монотонно возрастает. Например, при значении параметра **Интервал/Окно увеличения дискового буфера, минуты** равном 2 минуты сообщение об ошибке отобразится, если в течение 10 минут размер дискового буфера будет монотонно возрастать каждые 2 минуты (см. рис. ниже). 
`High enrichment queue`	**Интервал/Окно увеличения очереди обогащения, минуты**	Enrichment (обогащение) → Queue (очередь)	Сообщение об ошибке отображается, если в течение 10 минут с интервалом, заданным параметром **Интервал/Окно увеличения очереди обогащения, минуты**, значение метрики Queue монотонно возрастает. Например, при значении параметра **Интервал/Окно увеличения очереди обогащения, минуты** равном 3 минуты сообщение об ошибке отобразится, если в течение 10 минут очередь обогащения будет монотонно возрастать каждые три минуты. В случае, изображенном на рисунке ниже, сообщение об ошибке не отобразится, так как на девятой минуте значение метрики уменьшилось, поэтому последовательного монотонного возрастания нет. 

Сообщение об ошибке	Настраиваемые параметры для алертов	Метрика Kaspersky SIEM Cloud	Описание
`Enrichment errors increasing`	**Ошибки обогащения**	Enrichment (обогащение) → Errors (ошибки)	Сообщение об ошибке отображается, если значение метрики Errors (количество ошибок) возрастает в течение одной минуты. Вы можете включить или выключить отображение этого сообщения об ошибке с помощью параметра **Ошибки обогащения**.
`Connector log errors increasing`	**Отключить ошибки коннекторов**	IO (ввод-вывод) → Connector Errors (ошибки коннектора)	Сообщение об ошибке отображается, если значение метрики Connector Errors (количество ошибок) возрастает между последовательными опросами метрики решением VictoriaMetrics в течение одной минуты. Вы можете включить или выключить отображение этого сообщения об ошибке с помощью параметра **Отключить ошибки коннекторов**.

Срабатывание правил в режиме Интеллектуального обучения

В этом разделе представлена информация об обнаружениях, выполненных правилами Адаптивного контроля аномалий Kaspersky Endpoint Security для Windows на клиентских устройствах.

Правила обнаруживают аномальное поведение на клиентских устройствах и могут блокировать его. Если правила работают в режиме Интеллектуального обучения, они обнаруживают аномальное поведение и отправляют отчеты о каждом таком случае на Сервер администрирования Kaspersky SIEM Cloud. Вы можете просмотреть отчеты об анализе аномального поведения в разделе **Хранилища → Правила срабатываний в статусе Интеллектуальное обучение**. Вы можете подтвердить обнаружение как корректное или добавить его в исключения, после чего такой тип поведения не будет считаться аномальным.

Информация об обнаружениях хранится в журнале событий на Сервере администрирования (вместе с остальными событиями) и в отчете Адаптивный контроль аномалий.

Подробная информация об Адаптивном контроле аномалий, его правилах, их режимах и статусах приведена в справке Kaspersky Endpoint Security.

Просмотр списка обнаружений, выполненных с помощью правил Адаптивного контроля аномалий

Чтобы просмотреть список обнаружений, выполненных с помощью правил Адаптивного контроля аномалий:

1. В главном окне приложения перейдите в раздел **Хранилища → Правила срабатываний в статусе Интеллектуальное обучение**.

   В списке отображается следующая информация об обнаружении, выполняемая с помощью правил Адаптивного контроля аномалий:

   - **Группа администрирования**

     Имя группы администрирования, в которую включено устройство.

   - **Имя устройства**

     Имя клиентского устройства, на котором было применено правило.

   - **Имя**

     Имя правила, которое было применено.

- **Статус**

  Исключение – если администратор обработал это обнаружение и добавил его как исключение из правил. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

  Подтверждение – если администратор обработал это обнаружение и подтвердил его. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

  Пусто – если администратор не обработал обнаружение.

- **Имя пользователя**

  Имя пользователя клиентского устройства, запустившего процесс, который сгенерировал обнаружение.

- **Обработан**

  Дата обнаружения аномалии.

- **Путь исходного процесса**

  Путь к исходному процессу, то есть к процессу, выполнившему действие (подобную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного процесса**

  Хеш SHA256 исходного файла процесса (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь исходного объекта**

  Путь к объекту, который запустил процесс (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного объекта**

  Хеш SHA256 исходного файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого процесса**

  Путь к целевому процессу (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого процесса**

  Хеш SHA256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого объекта**

  Путь к целевому объекту (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого объекта**

  Хеш SHA256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

Чтобы просмотреть свойства каждого элемента:

1. В главном окне приложения перейдите в раздел **Операции** → **Хранилища**.

2. Перейдите по ссылке **Правила срабатываний в статусе Интеллектуальное обучение**.

3. В открывшемся окне выберите нужный объект.

4. Перейдите по ссылке **Свойства**.

   В открывшемся окне свойств объекта отображается информация выбранного элемента.

Вы можете подтвердить или добавить в исключения любой объект в списке, обнаруженный правилами Адаптивного контроля аномалий.

Чтобы подтвердить объект,

выберите один или несколько элементов в списке обнаружений и нажмите на кнопку **Подтвердить**.

Статус элементов будет изменен на **Подтверждается**.

Ваше подтверждение влияет на статистику, используемую правилами (подробную информацию см. в документации Kaspersky Endpoint Security для Windows).

Чтобы добавить объект в исключения,

выберите один или несколько элементов в списке обнаружений и нажмите на кнопку **Исключить**.

В результате запустится мастер добавления исключений. Следуйте далее указаниям мастера.

Если вы отклоните или подтвердите объект, он будет исключен из списка обнаружений после следующей синхронизации клиентского устройства с Сервером администрирования и больше не будет отображаться в списке.

Добавление исключений в правила Адаптивного контроля аномалий

Мастер добавления исключений позволяет добавлять исключения из правил Адаптивного контроля аномалий для Kaspersky Endpoint Security для Windows.

Чтобы запустить мастер добавления исключений в папке Адаптивный контроль аномалий:

1. В главном окне приложения перейдите в раздел **Хранилища → Правила срабатываний в статусе Интеллектуальное обучение**.

2. В открывшемся окне в контекстном меню одного или нескольких элементов в списке обнаружений нажмите на кнопку **Исключить**.

   За один раз можно добавить до 1000 исключений. Если вы выберете больше элементов и попытаетесь добавить их в исключения, появится сообщение об ошибке.

   В результате запустится мастер добавления исключений. Для продолжения работы мастера нажмите на кнопку **Далее**.

Отчеты администрирования и защиты

В этом разделе описывается, как использовать отчеты, управлять шаблонами пользовательских отчетов, использовать шаблоны для создания отчетов и создавать задачи рассылки отчетов.

Использование отчетов

Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

Отчеты доступны в OSMP Console в разделе **Мониторинг → Отчеты**.

По умолчанию отчеты включают информацию за последние 30 дней.

Kaspersky SIEM Cloud имеет по умолчанию набор отчетов для следующих категорий:

- **Состояние защиты**
- **Развертывание**
- **Обновление**
- **Статистика угроз**
- **Другие**

Вы можете создавать пользовательские шаблоны отчетов, редактировать шаблоны отчетов и удалять их.

Можно создавать отчеты на основе существующих шаблонов, экспортировать отчеты в файл и создавать задачи рассылки отчетов.

Шаблон отчета

Шаблоны отчетов используются для указания условий и данных, на основе которых будет сформирован отчет, а также для настройки периода формирования отчетов. Пользователи с ролью Главного администратора, Администратора тенанта, Аналитика второго уровня и Аналитика первого уровня могут создавать, изменять и удалять шаблоны отчетов. Отчеты, созданные с использованием шаблонов отчетов, отображаются на вкладке **Сформированные отчеты**.

Шаблоны отчетов доступны на вкладке **Шаблоны** раздела **Мониторинг → Отчеты → Обнаружение и реагирование**, где отображается таблица существующих шаблонов. В таблице содержится следующая информация:

- **Имя** – название шаблона отчета.

  Вы можете отсортировать шаблоны отчетов, нажав на значок сортировки ⌄ и в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

  Вы также можете искать шаблоны отчетов, используя поле **Поиск**, расположенное над таблицей.

При поиске шаблонов отчетов используются регулярные выражения.

- **Путь до ресурса** – название тенанта, которому принадлежит шаблон отчета.
- **Последнее обновление** – дата и время последнего обновления шаблона отчета.

  Вы можете отсортировать таблицу по этому столбцу, нажав на значок сортировки ⌄ и в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.
- **Создал** – имя пользователя, создавшего шаблон отчета.
- **Описание** – информация о шаблоне отчета, которую вы можете добавить при необходимости.
- **Теги** – теги для поиска шаблона отчета. Вы можете искать шаблоны отчетов, нажав на значок сортировки ⌄ в заголовке столбца, указав значение для поиска в поле **Поиск** или выбрав теги с помощью флажков.
- **Расписание** – периодичность, с которой отчеты должны формироваться по созданным шаблонам. Если расписание отчета не настроено, отображается значение выключено.
- **Последний отчет** – дата и время формирования последнего отчета по шаблону отчета.
- **Название пакета** – название пакета инструментов, предназначенного для обработки событий.
- **Отправить по электронной почте** – метка о настроенном уведомлении пользователей по почте о сформированных отчетах.

При необходимости вы можете настроить отображение столбцов в таблице, нажав на значок шестеренки ⚙.

После выбора шаблона отчета в списке вы можете нажать на значок меню ⋮, чтобы открыть раскрывающийся список с доступными действиями:

- **Показать зависимости** – используйте это действие, чтобы открыть окно графа зависимостей для выбранного шаблона отчета. При необходимости в окне графа можно скачать данные о зависимостях в формате SVG и настроить фильтры для показа зависимостей на графе.
- **Показать историю версий** – используйте это действие, чтобы посмотреть историю версий интересующего вас шаблона отчета. При необходимости в открывшейся боковой панели вы можете сравнить версии между собой и восстановить ранее использованную версию.
- **Запустить отчет** – используйте это действие, чтобы сформировать отчет. Созданные отчеты отображаются на вкладке **Сформированные отчеты**.
- **Показать все сформированные отчеты** – используйте это действие, чтобы посмотреть список всех отчетов, сформированных по выбранному шаблону отчета. При необходимости вы можете сохранить выбранный отчет в одном из поддерживаемых форматов или удалить отчет.
- **Редактировать расписание** – используйте это действие, чтобы настроить расписание для формирования отчетов и определить пользователей, которые должны получать уведомления по электронной почте о сформированных отчетах.

Вы также можете посмотреть доступный вам список шаблонов отчетов в разделе **Мониторинг** → **Ресурсы и сервисы** → **Список**. Для этого требуется выбрать **Шаблон отчетов** в столбце **Тип ресурса**.

Создание шаблона отчета

Чтобы создать шаблон отчета:

1. В главном окне приложения перейдите в раздел **Мониторинг → Отчеты**.
2. Нажмите на кнопку **Добавить**.

   В результате запустится мастер создания шаблона отчета. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Введите название отчета и выберите тип отчета.
4. На шаге мастера **Область действия** выберите набор клиентских устройств (групп администрирования, выборок устройств или всех сетевых устройств), данные о которых будут отображаться в отчетах, сформированных на основе этого шаблона.
5. На шаге мастера **Период отчета** укажите период, за который будет формироваться отчет. Доступные значения:

   - **От начальной даты до конечной даты**.
   - **От начальной даты до момента создания отчета**.
   - **За указанное число дней до момента создания отчета**.

   В некоторых отчетах эта страница может не отображаться.
6. Нажмите на кнопку **ОК**, чтобы завершить работу мастера.
7. Выполните одно из следующих действий:

   - Нажмите на кнопку **Сохранить и запустить**, чтобы сохранить новый шаблон отчета и запустить формирование отчета на его основе.

     Шаблон отчета будет сохранен. Отчет будет сформирован.
   - Нажмите на кнопку **Сохранить**, чтобы сохранить новый шаблон отчета.

     Шаблон отчета будет сохранен.

Созданный шаблон можно использовать для формирования и просмотра отчетов.

Просмотр и изменение свойств шаблона отчета

Вы можете просматривать и изменять основные свойства шаблона отчета, например, имя шаблона отчета или поля, отображаемые в отчете.

Чтобы просмотреть и изменить свойства шаблона отчета:

1. В веб-консоли перейдите в раздел **Мониторинг → Отчеты**.
2. Установите флажок напротив шаблона отчета, свойства которого вы хотите просмотреть и изменить.

   В качестве альтернативы можно сначала сформировать отчет, а затем нажать на кнопку **Изменить**.
3. Нажмите на кнопку **Открыть свойства шаблона отчета**.
4. Измените свойства шаблона отчета:

   - Вкладка **Общие**:

     - Название шаблона отчета
     - **Максимальное число отображаемых записей**

       Если этот параметр включен, количество отображаемых в таблице записей с подробными данными отчета не превышает указанное значение. Обратите внимание, что этот параметр не влияет на максимальное количество событий, которые вы можете включить в отчет при экспорте отчета в файл.

       Записи отчета сначала сортируются в соответствии с правилами, указанными в разделе **Поля → Детальные данные** свойств шаблона отчета, а затем сохраняется только первая часть результирующих записей. В заголовке таблицы с подробными данными отчета показано отображаемое количество записей и общее количество записей, соответствующее другим параметрам шаблона отчета.

       Если этот параметр выключен, в таблице с подробными данными отчета отображаются все записи. Не рекомендуется выключать этот параметр. Ограничение количества отображаемых записей отчета снижает нагрузку на систему управления базами данных и время, требуемое для формирования и экспорта отчета. В некоторых отчетах содержится слишком большое количество записей. В таких случаях просмотр и анализ всех записей может оказаться слишком трудоемким. Также на устройстве при формировании такого отчета может закончиться память. Это может привести к тому, что вам не удастся просмотреть отчет.

       По умолчанию параметр включен. По умолчанию указано значение 1000.

     - **Группа**

       Нажмите на кнопку **Параметры**, чтобы изменить набор клиентских устройств, для которых создается отчет. Для некоторых типов отчетов кнопка может быть недоступна. Реальные данные зависят от значений параметров, указанных при создании шаблона отчета.

     - **Период**

       Нажмите на кнопку **Параметры**, чтобы изменить период, за который будет сформирован отчет. Для некоторых типов отчетов кнопка может быть недоступна. Доступные значения:

       - **От начальной даты до конечной даты**.
       - **От начальной даты до момента создания отчета**.
       - **За указанное число дней до момента создания отчета**.

     - **Включать данные подчиненных и виртуальных Серверов администрирования**

       Если этот параметр включен, отчет содержит информацию с подчиненных и виртуальных Серверов администрирования, которые подчинены Серверу администрирования, для которого создан шаблон отчета.

Выключите этот параметр, если вы хотите просматривать данные только текущего Сервера администрирования.

По умолчанию параметр включен.

- **До уровня вложенности**

  Отчет содержит данные подчиненных и виртуальных Серверов администрирования, которые находятся под текущим Сервером администрирования на уровне вложенности ниже или равном указанному значению.

  По умолчанию указано значение 1. Вы можете изменить это значение, если вы хотите видеть в отчете информацию Серверов администрирования, расположенных на более низких уровнях вложенности дерева.

- **Интервал ожидания данных (мин)**

  Сервер администрирования, для которого создан шаблон отчета, ожидает данные от подчиненных Серверов администрирования в течение указанного времени для создания отчета. Если данные не получены от подчиненного Сервера администрирования в течение указанного интервала времени, отчет запускается в любом случае. Вместо фактических данных в отчете отображаются данные, полученные из кеша (если включен параметр **Кешировать данные с подчиненных Серверов администрирования**), или в противном случае **N/A** (Недоступно).

  По умолчанию время ожидания составляет 5 минут.

- **Кешировать данные с подчиненных Серверов администрирования**

  Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Переданные данные хранятся в кеше.

  Если Сервер администрирования не может получить данные подчиненного Сервера администрирования во время генерации отчета, в отчете отобразятся данные из кеша. В этом случае отображается дата, когда данные были переданы в кеш.

  Включение этого параметра позволяет просматривать информацию, полученную от подчиненных Серверов администрирования, даже если невозможно получить актуальные данные. Однако отображаемые данные могут быть устаревшими.

  По умолчанию параметр выключен.

- **Период обновления данных в кеше (ч)**

  Подчиненные Серверы администрирования через заданные интервалы времени (указанные в часах) передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Вы можете указать этот период в часах. Если установлено значение 0, данные передаются только во время генерации отчета.

  По умолчанию указано значение 0.

- **Передавать подробную информацию с подчиненных Серверов администрирования**

  В созданном отчете таблица с подробными данными включает информацию с подчиненных Серверов администрирования главного Сервера администрирования, для которого создан шаблон отчета.

  Если этот параметр включен, то замедляется создание отчета и увеличивается трафик между Серверами администрирования. Однако вы можете просмотреть все данные в одном отчете.

  Чтобы не включать этот параметр, вы можете проанализировать данные отчета для нахождения неисправного подчиненного Сервера администрирования, а затем сформировать этот же отчет только для него.

  По умолчанию параметр выключен.

- Вкладка **Поля**

  Выберите поля, которые будут отображаться в отчете. С помощью кнопок **Вверх** и **Вниз** измените порядок отображения полей. С помощью кнопок **Добавить** и **Изменить** укажите, будет ли информация в отчете фильтроваться или сортироваться по выбранным полям.

  В разделе **Фильтры детальных полей** вы также можете нажать на кнопку **Преобразовать фильтры**, чтобы начать использовать расширенный формат фильтрации. Этот формат позволяет комбинировать условия фильтрации, указанные в различных полях, с помощью логического ИЛИ. После нажатия на кнопку **Преобразовать фильтры**, справа открывается панель. Нажмите на кнопку **Преобразовать фильтры**, подтверждающую отзыв лицензии. Теперь вы можете определить преобразованный фильтр с условиями из раздела **Детальные данные**, которые применяются с помощью логического ИЛИ.

  > Преобразование отчета в формат, поддерживающий сложные условия фильтрации, сделает его несовместимым с предыдущими версиями Kaspersky Security Center (11 и ниже). Также в преобразованном отчете не будет данных с подчиненных Серверов администрирования с несовместимыми версиями.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.
6. Закройте окно **Редактирование отчета <Название отчета>**.

Измененный шаблон отчета появится в списке шаблонов отчетов.

Удаление шаблонов отчетов

Чтобы удалить шаблоны отчетов:

1. В главном окне приложения перейдите в раздел **Мониторинг → Отчеты**.
2. Установите флажки напротив шаблонов отчетов, которые требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**, чтобы подтвердить свой выбор.

Выбранные шаблоны отчетов будут удалены. Если эти шаблоны отчетов были включены в задачи рассылки отчетов, они также будут удалены из этих задач.

Универсальность шаблона отчетов

Шаблон отчета в Kaspersky SIEM Cloud считается универсальным, если создается в тенанте Shared. Шаблоны отчетов, созданные в других тенантах, являются неуниверсальными.

Для работы с универсальным шаблоном отчета у пользователя должны быть следующие роли:

- Для создания, изменения параметров и удаления нужна роль Редактирование общих ресурсов. При наличии такой роли пользователь получает доступ ко всем общим ресурсам.

  Если роль пользователя предполагает работу с ресурсами КИИ, то признак КИИ может установить любой пользователь с ролью Редактирование общих ресурсов.

- Для просмотра списка универсальных шаблонов отчетов нужна роль Чтение общих ресурсов. При наличии таких прав пользователь получает доступ на чтение всех общих ресурсов.

Виджеты в универсальном шаблоне отчета отображаются с учетом следующего:

- Данные виджетов для тенантов отображаются в соответствии с доступом пользователя к тенантам, глобальным фильтром тенантов и конфигурацией шаблона отчетов или виджета.

- Данные виджетов при изменении параметров шаблона отчета можно посмотреть с помощью кнопки **Обновить предпросмотр**.

- Данные виджетов по событиям поступают из базы данных в соответствии с параметрами набора пространств пользователя. Если при формировании отчета оказывается, что у пользователя нет доступа к пространствам одного или нескольких тенантов, Kaspersky SIEM Cloud сформирует пустой отчет и отобразится сообщение о невозможности предоставления других результатов из-за отсутствия доступа к нужным пространствам.

- Данные виджетов в отчете могут формироваться с учетом КИИ или без учета КИИ. Для доступа к отчетам, в которых данные рассчитывались с учетом КИИ, у пользователя должна быть роль Доступ к КИИ.

- К универсальным отчетам применимы ограничения для виджетов активных листов и контекстных таблиц.

Экспорт отчета в файл

Вы можете сохранить один или несколько отчетов в форматах XML, HTML или PDF. Open Single Management Platform позволяет экспортировать до 10 отчетов в файлы указанного формата одновременно.

Формат PDF доступен только в том случае, если вы подключены к подчиненному Серверу администрирования в Консоли OSMP.

Чтобы экспортировать отчет в файл:

1. В веб-консоли перейдите в раздел **Мониторинг** → **Отчеты**.

2. Выберите отчеты, которые вы хотите экспортировать.

   Если вы выберете более десяти отчетов, кнопка **Экспортировать отчет** будет неактивна.

3. Нажмите на кнопку **Экспортировать отчет**.

4. В открывшемся окне настройте следующие параметры экспорта:

   - **Имя**

     Если вы выбрали один отчет для экспорта, укажите имя файла отчета.

     Если вы выбрали несколько отчетов, имена файлов отчетов будут совпадать с именами выбранных шаблонов отчетов.

- **Максимальное количество записей**.

  Укажите максимальное количество записей, которые будут включены в файл отчета. По умолчанию указано значение 10 000.

  Вы можете экспортировать отчет с неограниченным количеством записей. Обратите внимание, что если ваш отчет содержит большое количество записей, время, необходимое для создания и экспорта отчета, увеличивается.

- **Формат файла**.

  Выберите формат файла отчета: XML, HTML, или PDF. При экспорте нескольких отчетов все выбранные отчеты сохраняются в указанном формате в виде отдельных файлов.

  > Формат PDF доступен только в том случае, если вы подключены к подчиненному Серверу администрирования в Консоли OSMP.

  > Инструмент wkhtmltopdf необходим для преобразования отчета в формат PDF. При выборе параметра PDF подчиненный Сервер администрирования проверяет, установлена ли на устройстве утилита wkhtmltopdf. Если инструмент не установлен, приложение выводит сообщение о том, что его необходимо установить на устройство с Сервером администрирования. Установите инструмент вручную, а затем переходите к следующему шагу.

5. Нажмите на кнопку **Экспортировать отчет**.

Отчет будет сохранен в файл в указанном формате.

Генерация и просмотр отчета

Чтобы сформировать и просмотреть отчет:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Отчеты**.

2. Нажмите на имя шаблона отчета, который вы хотите использовать для создания отчета.

   Отображается сгенерированный отчет с использованием выбранного шаблона.

> Данные отчета отображаются в соответствии с языком локализации Сервера администрирования.

> В сформированных отчетах некоторые шрифты могут некорректно отображаться на диаграммах. Чтобы избежать этого, установите библиотеку fontconfig. Также убедитесь, что в операционной системе установлены шрифты, соответствующие языковому стандарту вашей операционной системы.

В отчете отображаются следующие данные:

- На вкладке **Сводная информация**:
  - тип и название отчета, его краткое описание и отчетный период, а также информация о том, для какой группы устройств создан отчет;
  - графическая диаграмма с наиболее характерными данными отчета;
  - сводная таблица с вычисляемыми показателями отчета.
- На вкладке **Подробнее** отобразится таблица с подробными данными отчета.

Создание задачи рассылки отчета

Можно создать задачу рассылки выбранных отчетов.

Чтобы создать задачу рассылки отчета:

1. В главном окне приложения перейдите в раздел **Мониторинг → Отчеты**.
2. Установите флажки рядом с шаблонами отчетов, на основе которых вы хотите сформировать задачу рассылки отчетов.
3. Нажмите на кнопку **Создать задачу рассылки отчетов**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
4. На шаге мастера **Параметры новой задачи** введите название задачи.

   Название задачи по умолчанию – **Рассылка отчетов.** Если задача с таким названием уже существует, к названию задачи добавляется порядковый номер (<N>).
5. На шаге мастера **Конфигурация отчета** укажите следующие параметры:
   a. Шаблоны отчетов, рассылаемых задачей.
   b. Формат отчета: HTML, XLS или PDF.

      Инструмент wkhtmltopdf необходим для преобразования отчета в формат PDF. При выборе параметра PDF Сервер администрирования проверяет, установлена ли на устройстве утилита wkhtmltopdf. Если инструмент не установлен, приложение выводит сообщение о том, что его необходимо установить на устройство с Сервером администрирования. Установите инструмент вручную, а затем переходите к следующему шагу.
   c. Будут ли отчеты рассылаться по электронной почте, а также параметры почтовых уведомлений.

      Вы можете указать до 20 адресов электронной почты. Чтобы разделить адреса электронной почты, нажмите на клавишу **Enter**. Вы также можете вставить список адресов электронной почты, разделенных запятыми, и нажать на клавишу **Enter**.
6. На шаге мастера **Настройка расписания запуска задачи** выберите расписание запуска задачи.

   Доступны следующие варианты расписания запуска задачи:
   - **Вручную**

     Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию выбран этот вариант.

- **Каждые N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые 6 часов, начиная с текущих системной даты и времени.

- **Каждые N дней**

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются приложением, для которого вы создаете задачу.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

  По умолчанию задача запускается каждую пятницу в текущее системное время.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **В указанные дни**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию указано время 18:00 и не выбраны дни месяца.

  > Обратите внимание, что вы выбираете порядковый номер дня недели в месяце, а не конкретную дату в месяце или номер недели (первая, вторая неделя месяца). Например, если вы выберите ячейку **Вт** в строке **Первая**, в этом случае задача будет запускаться каждый первый вторник каждого нового месяца.

  Вы можете выбрать несколько дней недели.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы приложений, которые будут отслеживать вирусные атаки. Доступны следующие типы приложений:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы приложений.

  Вы можете запускать разные задачи в зависимости от типа приложения безопасности, сообщающего о вирусной атаке. В этом случае удалите выбор типов приложений, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам. Например, вы можете запустить задачу *Управление устройствами* с помощью параметра **Включить устройство** и после ее завершения запустить задачу *Поиск вирусов*, как запускающую задачу.

  Вам нужно выбрать запускающую задачу из таблицы и статус, с которым эта задача должна завершиться (**Завершена успешно** или **Сбой**).

  При необходимости вы можете искать, сортировать и фильтровать задачи в таблице следующим образом:

  - Введите название задачи в поле поиска, чтобы выполнить поиск задачи по названию.
  - Нажмите на значок сортировки, чтобы отсортировать задачи по имени.

    По умолчанию задачи отсортированы в алфавитном порядке по возрастанию.
  - Нажмите на значок фильтра и в открывшемся окне отфильтруйте задачи по группам, после чего нажмите на кнопку **Применить**.

7. На этом шаге мастера настройте другие параметры расписания запуска задачи:

- В разделе **Расписание задачи** проверьте или перенастройте ранее выбранное расписание и установите период, дни месяца или недели, задайте условие вирусной атаки или выполнение другой задачи в качестве запуска задачи. В этом разделе также можно указать время запуска, если выбрано подходящее расписание.
- В разделе **Дополнительные параметры** укажите следующие параметры:

  - **Запускать пропущенные задачи**

    Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

    Если параметр включен, при очередном запуске приложения "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию. Для расписания **Вручную**, **Один раз** и **Немедленно** задачи выполняются только на тех клиентских устройствах, которые видны в сети. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задачи**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр включен.

- **Использовать автоматическую случайную задержку запуска задачи в интервале**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

- **Остановить, если задача выполняется дольше**

  По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

  Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

  По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

8. На шаге мастера **Выбор учетной записи для запуска задачи** укажите учетные данные учетной записи, которая используется для запуска задачи.

9. Если требуется изменить другие параметры задачи после ее создания, на шаге мастера **Завершение создания задачи** включите параметр **Открыть окно свойств задачи после ее создания**. По умолчанию параметр включен.

10. Нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

Будет создана задача отправки отчета. Если параметр **Открыть окно свойств задачи после ее создания** включен, откроется окно параметров задачи.

Отчеты обнаружения и реагирования

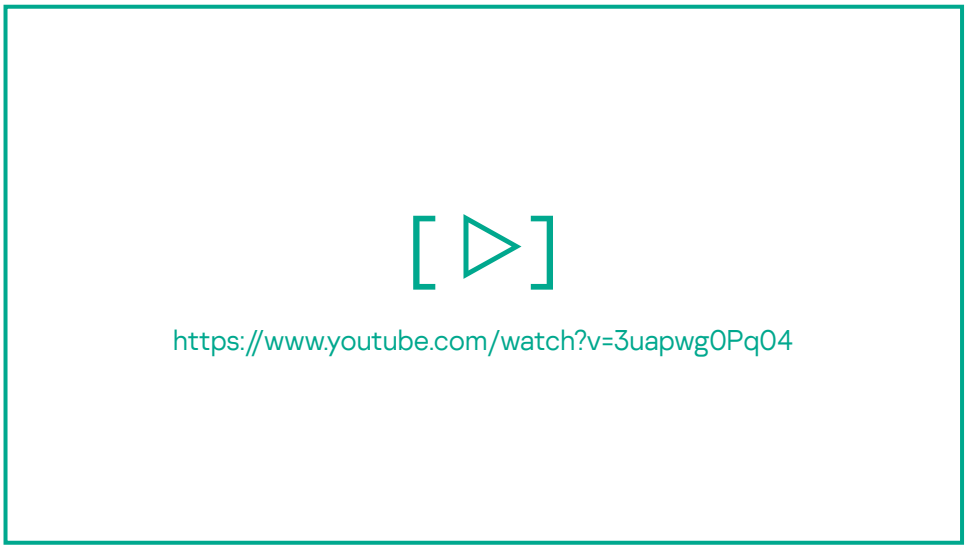
Вы можете настроить регулярное формирование отчетов о состоянии процессов и объектов в Kaspersky SIEM Cloud.

Отчеты формируются с помощью *шаблонов отчетов*. Шаблоны отчетов находятся в разделе **Мониторинг** → **Отчеты** → **Обнаружение и реагирование** на вкладке **Шаблоны**.

Сформированные отчеты хранятся в разделе **Мониторинг** → **Отчеты** → **Обнаружение и реагирование** на вкладке **Сформированные отчеты**.

Чтобы сохранять сформированные отчеты в форматах HTML и PDF необходимо установить требуемые пакеты на устройстве с Ядром Kaspersky SIEM Cloud.

При развертывании Kaspersky SIEM Cloud в отказоустойчивом варианте временная зона сервера Ядра Kaspersky SIEM Cloud и время в браузере пользователя могут различаться. Это различие проявляется в расхождении времени, которое проставляется в отчетах, сформированных по расписанию, и данных, которые пользователь может экспортировать из виджетов. Чтобы избежать расхождения, рекомендуется настроить расписание формирования отчетов с учетом разницы временной зоны пользователей и временем UTC.



https://www.youtube.com/watch?v=3uapwg0Pq04

Шаблон отчета

Шаблоны отчетов используются для указания условий и данных, на основе которых будет сформирован отчет, а также для настройки периода формирования отчетов. Пользователи с ролью Главного администратора, Администратора тенанта, Аналитика второго уровня и Аналитика первого уровня могут создавать, изменять и удалять шаблоны отчетов. Отчеты, созданные с использованием шаблонов отчетов, отображаются на вкладке **Сформированные отчеты**.

Шаблоны отчетов доступны на вкладке **Шаблоны** раздела **Мониторинг** → **Отчеты** → **Обнаружение и реагирование**, где отображается таблица существующих шаблонов. В таблице содержится следующая информация:

- **Имя** – название шаблона отчета.

  Вы можете отсортировать шаблоны отчетов, нажав на значок сортировки ⌄ и в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

  Вы также можете искать шаблоны отчетов, используя поле **Поиск**, расположенное над таблицей.

  При поиске шаблонов отчетов используются регулярные выражения.

- **Путь до ресурса** – название тенанта, которому принадлежит шаблон отчета.

- **Последнее обновление** – дата и время последнего обновления шаблона отчета.

  Вы можете отсортировать таблицу по этому столбцу, нажав на значок сортировки ⌄ и в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

- **Создал** – имя пользователя, создавшего шаблон отчета.

- **Описание** – информация о шаблоне отчета, которую вы можете добавить при необходимости.

- **Теги** – теги для поиска шаблона отчета. Вы можете искать шаблоны отчетов, нажав на значок сортировки ⌄ в заголовке столбца, указав значение для поиска в поле **Поиск** или выбрав теги с помощью флажков.

- **Расписание** – периодичность, с которой отчеты должны формироваться по созданным шаблонам. Если расписание отчета не настроено, отображается значение `выключено`.

- **Последний отчет** – дата и время формирования последнего отчета по шаблону отчета.

- **Название пакета** – название пакета инструментов, предназначенного для обработки событий.

- **Отправить по электронной почте** – метка о настроенном уведомлении пользователей по почте о сформированных отчетах.

При необходимости вы можете настроить отображение столбцов в таблице, нажав на значок шестеренки ⚙.

После выбора шаблона отчета в списке вы можете нажать на значок меню ⋮, чтобы открыть раскрывающийся список с доступными действиями:

- **Показать зависимости** – используйте это действие, чтобы открыть окно графа зависимостей для выбранного шаблона отчета. При необходимости в окне графа можно скачать данные о зависимостях в формате SVG и настроить фильтры для показа зависимостей на графе.

- **Показать историю версий** – используйте это действие, чтобы посмотреть историю версий интересующего вас шаблона отчета. При необходимости в открывшейся боковой панели вы можете сравнить версии между собой и восстановить ранее использованную версию.

- **Запустить отчет** – используйте это действие, чтобы сформировать отчет. Созданные отчеты отображаются на вкладке **Сформированные отчеты**.

- **Показать все сформированные отчеты** – используйте это действие, чтобы посмотреть список всех отчетов, сформированных по выбранному шаблону отчета. При необходимости вы можете сохранить выбранный отчет в одном из поддерживаемых форматов или удалить отчет.

- **Редактировать расписание** – используйте это действие, чтобы настроить расписание для формирования отчетов и определить пользователей, которые должны получать уведомления по электронной почте о сформированных отчетах.

Вы также можете посмотреть доступный вам список шаблонов отчетов в разделе **Мониторинг → Ресурсы и сервисы → Список**. Для этого требуется выбрать **Шаблон отчетов** в столбце **Тип ресурса**.

Создание шаблона отчета

Чтобы создать шаблон отчета:

1. В веб-консоли перейдите в один из следующих разделов:

   - **Мониторинг** → **Отчеты** → **Обнаружение и реагирование** → **Шаблоны**.

   - **Мониторинг** →**Ресурсы и сервисы** → **Список**.

     Если вы выбрали этот раздел, для удобства отображения объектов вы можете выбрать **Шаблон отчетов** в столбце таблицы **Тип ресурса**.

2. В зависимости от выбранного раздела выполните одно из следующих действий:

   - В разделе **Мониторинг** → **Отчеты** → **Обнаружение и реагирование** → **Шаблоны** нажмите на кнопку **Создать**, расположенную над таблицей со списком шаблонов отчетов.

   - В разделе **Мониторинг** →**Ресурсы и сервисы** → **Список** нажмите на кнопку **Создать** и выберите **Шаблон отчетов** в списке ресурсов.

3. В открывшемся окне укажите уникальное название шаблона отчета. Название должно содержать от 1 до 128 символов Юникода.

   Пользовательские шаблоны отчетов не могут иметь названия предустановленных шаблонов отчетов в тенанте Main.

   При попытке создать шаблон отчетов с названием предустановленного шаблона отчетов или присвоить пользовательскому шаблону отчетов имя предустановленного шаблона отчетов в тенанте Main вернется ошибка. В других тенантах, помимо тенанта Main, можно создать или дублировать пользовательский шаблон отчетов с именем предустановленного шаблона отчетов. Рекомендуется использовать пользовательские имена для пользовательских шаблонов отчетов.

4. При необходимости в раскрывающемся списке **Временной интервал** выберите период, по которому требуется аналитика, одним из следующих способов:

   - Если вы хотите указать точную дату, в календаре слева выберите даты начала и окончания периода и нажмите на кнопку **Применить**.

     Вы можете выбрать дату до текущей включительно. Формат даты и времени зависит от параметров вашего браузера. Если в поле **Дата от** или **Дата до** есть значение и вы не меняли вручную значение времени, при выборе даты в календаре в поле **Дата от** автоматически подставится время 00:00:00.000, а в поле **Дата до** – 23:59:59.999. Если вы вручную удалили значение в поле **Дата от** или **Дата до**, при выборе даты в календаре в поле автоматически подставится текущее время. После того как вы выберите значение в одном из полей, фокус переключается на другое поле. Если в поле **Дата до** вы выбираете значение, которое меньше значения в поле **Дата от**, это меньшее значение будет автоматически подставлено в поле **Дата от**.

   - Если вы хотите указать относительный период, выберите один из доступных периодов в списке **Относительный период** справа.

     Период рассчитывается относительно настоящего времени.

   - Если вы хотите задать пользовательский период, укажите или измените значение вручную в полях **Дата от** и **Дата до**.

     Вы можете указать точные дату и время в формате **DD.MM.YYYY HH:mm:ss.SSS** для русской локализации и **YYYY-MM-DD HH:mm:ss.SSS** для английской локализации или период относительно текущего времени в виде формулы. При необходимости вы также можете комбинировать эти способы. Если при вводе точной даты вы не указали миллисекунды, значение 000 подставляется автоматически. Если вы вручную изменили время в полях **Дата от** или **Дата до**, при переключении даты в календаре значение времени не меняется.

В формулах относительного периода используйте параметр now для обозначения текущих даты и времени, а также: символы "+" (только в поле **Дата до**), "-", "/" (округление до ближайшего) и единицы изменения времени **y** (год), **M** (месяц), **w** (неделя), **d** (день), **h** (час), **m** (минута), **s** (секунда). Например, вы можете указать период **now-5d**, чтобы получить данные за последние пять дней, или **now/w**, чтобы получить данные с начала первого дня текущей недели (00:00:00:000 в UTC) до текущего времени **now**.

Поле **От** является обязательным, и его значение не может превышать значение, установленное в поле **До**, а также не может быть меньше 01.01.1970 (при указании точной даты или относительного периода). Значение в поле **Дата до** не должно быть меньше значения, установленного в поле **Дата от**. Если вы не укажете значение в поле **До**, параметр **now** указывается автоматически.

По умолчанию выбран относительный период **1 день (now-1d)**. Границы периода включаются. Например, для периода **Сегодня** отобразятся события с начала сегодняшнего дня 00:00:00:000 до текущего времени **now** включительно, а для периода **Вчера** – с начала вчерашнего дня 00:00:00:000 до 00:00:00:000 сегодняшнего дня.

Время в Kaspersky SIEM Cloud хранится в UTC, но в интерфейсе оно конвертируется в соответствии с часовым поясом вашего браузера. Это нужно учитывать для относительных периодов **Сегодня**, **Вчера**, **Эта неделя** и **Этот месяц**. Например, если в браузере установлен часовой пояс UTC+3 и вы выбрали период отображения данных **Сегодня**, данные будут отображаться за период с 03:00:00.000 до текущего времени, а не с 00:00:00.000.

Если при выборе относительного периода **Сегодня**, **Вчера**, **Эта неделя** или **Этот месяц** вы хотите отобразить данные в соответствии с вашим часовым поясом, вам нужно вручную добавить сдвиг по времени в поля **Дата от** и **Дата до** (если указано значение кроме now), прибавив или убавив необходимое количество часов. Например, если в браузере установлен часовой пояс UTC+3 и вы хотите отобразить данные за период **Вчера**, вам нужно изменить значение в поле **Дата от** на **now-1d/d-3h**, а в поле **Дата до** – на **now/d-3h**. Если же вы хотите отобразить данные за период **Сегодня**, вам нужно изменить значение только в поле **Дата от** на **now/d-3h**.

Если вам нужны результаты до 23:59:59:999 вчерашнего дня в UTC, то используйте SQL-запрос с фильтром по Timestamp или укажите точные дату и время.

5. При необходимости в поле **Срок хранения** укажите, в течение какого времени следует хранить сформированные по этому шаблону отчеты.

   Значение по умолчанию – 3 месяца.

6. При необходимости в раскрывающемся списке **Теги** выберите нужные теги для шаблона отчета.

7. При необходимости добавьте описание шаблона отчета.

8. При необходимости включите переключатель **Скрыть заголовок**.

9. При необходимости включите переключатель **Не отправлять пустые отчеты**.

10. Нажмите на кнопку **Сохранить**.

11. В открывшемся окне при необходимости можно поменять логотип шаблона отчетов, нажав на ссылку **Загрузите файл**. В окне загрузки укажите файл изображения для логотипа. Изображение должно быть в формате JPG, PNG или GIF и размером не более 3 МБ.

    Добавленный логотип будет отображаться в отчете вместо логотипа Kaspersky SIEM Cloud.

12. Нажмите на кнопку **Добавить виджет** и выберите требуемый виджет. В открывшемся окне настройте параметры выбранного виджета.

Вы можете добавить несколько виджетов. Виджеты можно перетаскивать по окну с помощью значка перетаскивания (⠿), расположенного рядом с левым верхним углом виджета. Если вам необходимо изменить размер виджета, вы можете сделать это с помощью значка растяжения (⤡), который появляется при наведении указателя мыши на правый нижний угол виджета.

Для виджетов с типами графиков **Круговая диаграмма**, **Столбчатая диаграмма**, **Линейная диаграмма**, **Счетчик** и **Календарная диаграмма** существуют следующие ограничения:

- В запросах `SELECT` можно использовать поля расширенной схемы событий с типами `Строка`, `Число` и `Число с плавающей точкой`.
- В запросах `WHERE` можно использовать поля расширенной схемы событий со всеми типами (`Строка`, `Число`, `Число с плавающей точкой`, `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой`).

Для виджетов с типом графика `Таблица` в запросах `SELECT` можно использовать поля расширенной схемы событий со всеми типами (`Строка`, `Число`, `Число с плавающей точкой`, `Массив строк`, `Массив чисел` и `Массив чисел с плавающей точкой`).

Нажав на значок меню ⋮ в правом верхнем углу виджета, вы можете выполнять следующие действия с виджетами:

- изменять параметры виджетов;
- создавать копии виджетов;
- удалять виджеты;
- загружать данные виджетов в формате .csv.

13. Нажмите на кнопку **Создать**.

    Новый шаблон отчета создан и отображается в OSMP Console на вкладках **Мониторинг** → **Отчеты** → **Обнаружение и реагирование** → **Шаблоны** и **Мониторинг** →**Ресурсы и сервисы** → **Список**. Вы можете сформировать этот отчет вручную. Если вы хотите, чтобы отчеты создавались автоматически, нужно настроить расписание.

Настройка расписания отчетов

Чтобы настроить расписание отчетов:

1. В веб-консоли перейдите в раздел **Мониторинг** → **Отчеты** → **Обнаружение и реагирование** → **Шаблоны**.
2. В таблице со списком шаблонов отчета выберите шаблон отчета и нажмите на значок меню ⋮.
3. В раскрывающемся списке выберите **Редактировать расписание**.
4. Если вы хотите, чтобы отчет формировался регулярно:
   a. Включите переключатель **Отправить отчет по расписанию**.
   b. В группе параметров **Повторять каждый** укажите периодичность формирования отчетов.

      Периодичность формирования отчетов можно указать по дням, неделям, месяцам или годам. В зависимости от выбранного периода требуется задать время, день недели, число месяца или дату формирования отчета.

c. В поле **Время** укажите время, когда должен быть сформирован отчет.

d. В раскрывающемся списке **Часовой пояс** выберите часовой пояс для определения времени отправки отчета.

5. В блоке **Настройки уведомлений** укажите следующие параметры:

a. В раскрывающемся списке **Шаблон уведомления** выберите форму уведомления, которое будет направляться пользователю по расписанию.

b. В группе настроек **Отправить** нажмите **Добавить**.

c. В открывшемся окне добавьте группу пользователей для отправки отчета и выберите нужный вам формат. Для этого выполните следующие действия:

- В раскрывающемся списке **Адреса электронной почты** выберите адреса электронной почты получателей отчета.
- В раскрывающемся списке **Формат** выберите формат отчета. Для выбора доступны следующие форматы: PDF, HTML, CSV, разделенный CSV, Excel.

Вы можете добавить несколько групп пользователей для отправки отчета, нажав на кнопку **Добавить группу**.

Отчеты будут отправлены по указанным адресам каждый раз, когда вы сформируете отчет вручную или Kaspersky SIEM Cloud сформирует отчет автоматически по расписанию.

> Чтобы сформированные отчеты можно было отправлять по электронной почте, нужно настроить SMTP-соединение.

Если получатели, которым отчет пришел на электронную почту, являются пользователями Kaspersky SIEM Cloud, они смогут скачать отчет или просмотреть отчет по ссылкам из письма. Если адресаты не являются пользователями Kaspersky SIEM Cloud, переход по ссылкам будет доступен, но авторизоваться в Kaspersky SIEM Cloud адресаты не смогут, поэтому им будут доступны только вложения.

Рекомендуется просматривать отчеты в формате HTML по ссылкам в веб-интерфейсе, поскольку при некоторых значениях разрешения экрана HTML-отчет из вложения может отображаться некорректно.

Вы можете отправить письмо без вложений, тогда получателям будут доступны отчеты только по ссылкам и только с аутентификацией в Kaspersky SIEM Cloud, без ограничений по ролям или тенантам.

d. Нажмите на кнопку **Добавить**.

6. Нажмите на кнопку **Сохранить**.

Расписание отчетов настроено.

Изменение шаблона отчета

Чтобы изменить шаблон отчета:

1. В веб-консоли перейдите в один из следующих разделов:

   - **Мониторинг → Отчеты → Обнаружение и реагирование → Шаблоны**.
   - **Мониторинг → Ресурсы и сервисы → Список**.

     Если вы выбрали этот раздел, для удобства отображения объектов вы можете выбрать **Шаблон отчетов** в столбце таблицы **Тип ресурса**.

2. В зависимости от выбранного раздела выполните одно из следующих действий:

   - В разделе **Отчеты → Обнаружение и реагирование → Шаблоны** нажмите имя шаблона отчетов в таблице со списком шаблонов отчетов.
   - В разделе **Ресурсы и сервисы → Список** нажмите на значок изменения параметров (⧉) рядом с именем шаблона отчетов в списке ресурсов.

   Откроется окно **Изменить шаблон**.

   Это окно также можно открыть на вкладке **Отчеты → Обнаружение и реагирование → Сформированные отчеты**, выбрав существующий отчет и нажав на кнопку **Редактировать шаблон отчета**.

3. Внесите необходимые изменения:

   - Измените название шаблона отчета.
   - Измените список тенантов, которые передают данные для отчета.
   - Нажмите на кнопку **Параметры** для изменения периода получения аналитических данных, срока хранения, тегов и описания шаблона отчета.
   - Нажмите на кнопку **Добавить виджет** для добавления виджета в шаблон отчета.
   - Нажмите на значок меню (⋮) для просмотра списка отчетов, сформированных по этому шаблону, или для удаления шаблона отчета.
   - Измените логотип отчета, загрузив его по ссылке **Загрузите файл**. Если в шаблоне уже есть логотип, его предварительно потребуется удалить.
   - Измените расположение виджетов, перетаскивая их.
   - Измените размер виджетов с помощью значка растяжения (⤡), который появляется при наведении указателя мыши на виджет.
   - С помощью значка меню (⋮) на виджете измените параметры виджетов, создайте копии виджетов, удалите виджеты или загрузите данные виджетов в формате CSV.

4. Нажмите на кнопку **Сохранить**.

Шаблон отчета изменен и отображается в веб-консоли в разделах **Мониторинг → Отчеты → Обнаружение и реагирование → Шаблоны** и **Мониторинг → Ресурсы и сервисы → Список**.

Копирование шаблона отчета

Чтобы создать копию шаблона отчета:

1. В веб-консоли перейдите в один из следующих разделов:

   - **Мониторинг → Отчеты → Обнаружение и реагирование → Шаблоны**.
   - **Мониторинг → Ресурсы и сервисы → Список**.

     Если вы выбрали этот раздел, для удобства отображения объектов вы можете выбрать **Шаблон отчетов** в столбце таблицы **Тип ресурса**.

2. В таблице выберите шаблон отчета и нажмите на кнопку **Дублировать**, расположенную над таблицей.
3. В открывшемся окне укажите название шаблона отчета. При копировании шаблона отчета в названии отчета появляется упоминание о копировании.
4. При необходимости измените следующие параметры:

   - Период формирования отчета.
   - Срок хранения отчета.
   - Теги шаблона отчета.
   - Описание шаблона отчета.

5. Нажмите на кнопку **Сохранить**.

Шаблон отчета изменен и отображается в веб-консоли в разделах **Мониторинг → Отчеты → Обнаружение и реагирование → Шаблоны** и **Мониторинг → Ресурсы и сервисы → Список**.

Удаление шаблона отчета

Чтобы удалить шаблон отчета:

1. В веб-консоли перейдите в один из следующих разделов:

   - **Мониторинг → Отчеты → Обнаружение и реагирование → Шаблоны**.
   - **Мониторинг → Ресурсы и сервисы → Список**.

     Если вы выбрали этот раздел, для удобства отображения объектов вы можете выбрать **Шаблон отчетов** в столбце таблицы **Тип ресурса**.

2. В таблице шаблонов отчетов с помощью флажка выберите шаблон отчета и нажмите на кнопку **Удалить**, расположенную над таблицей.

   Откроется окно подтверждения.

3. Выполните одно из следующих действий:

   - Если вы хотите удалить только шаблон отчета, нажмите на кнопку **Удалить**.
   - Если вы хотите удалить шаблон отчета и все отчеты, сформированные с помощью этого шаблона, нажмите **Удалить с отчетами**.

Шаблон отчета удален.

Экспорт и импорт шаблона отчета

Чтобы экспортировать шаблон отчета:

1. В веб-консоли перейдите в один из следующих разделов:

   - **Мониторинг → Отчеты → Обнаружение и реагирование → Шаблоны**.
   - **Мониторинг → Ресурсы и сервисы → Список**.

     Если вы выбрали этот раздел, для удобства отображения объектов вы можете выбрать **Шаблон отчетов** в столбце таблицы **Тип ресурса**.

   Откроется окно со списком всех шаблонов отчетов, доступных вам в Kaspersky SIEM Cloud.

2. С помощью флажка выберите шаблон отчета для экспорта.
3. Нажмите на кнопку **Экспортировать**, расположенную над таблицей со списком шаблонов отчетов.
4. В открывшейся боковой панели выполните следующие действия:

   a. Укажите пароль к файлу с экспортируемыми ресурсами. Пароль должен удовлетворять следующим требованиям:

      - длина минимум 16 символов;
      - хотя бы один символ в нижнем регистре;
      - хотя бы один символ в верхнем регистре;
      - хотя бы одна цифра;
      - хотя бы один специальный символ.

   b. В раскрывающемся списке **Тенант** выберите тенант, из которого вы хотите экспортировать выбранные ресурсы.

   c. С помощью флажков укажите ресурсы, которые вы хотите экспортировать.

      Если вы установите флажок **Все ресурсы**, экспортироваться будут все ресурсы, находящиеся в папках выбранного тенанта.

5. Нажмите на кнопку **Экспортировать**.

При экспорте шаблонов отчета необходимо учитывать следующее:

- Шаблоны отчетов экспортируются без информации о тенантах, хранилищах и пространствах.
- Виджеты шаблона отчета также экспортируются без информации о тенантах, хранилищах и пространствах.

Чтобы импортировать шаблон отчета:

1. В веб-консоли перейдите в один из следующих разделов:
   - **Мониторинг → Отчеты → Обнаружение и реагирование → Шаблоны**.
   - **Мониторинг → Ресурсы и сервисы → Список**.

     Если вы выбрали этот раздел, для удобства отображения объектов вы можете выбрать **Шаблон отчетов** в столбце таблицы **Тип ресурса**.

   Откроется окно со списком всех шаблонов отчетов, доступных вам в Kaspersky SIEM Cloud.
2. С помощью флажка выберите шаблон отчета для импорта.
3. Нажмите на кнопку **Импортировать**, расположенную над таблицей со списком ресурсов.
4. В открывшейся боковой панели в раскрывающемся списке **Тенант** выберите тенант, в который вы хотите импортировать шаблон отчета.
5. Выберите источник импорта: **Файл** или **Репозиторий**.
6. В зависимости от выбранного источника импорта, выполните следующие шаги:
   a. Если вы выбрали **Файл** в качестве источника импорта, выполните следующие действия:
      - Укажите пароль к импортируемому файлу.
      - С помощью кнопки **Выбрать файл** выберите файл для импорта.
      - С помощью флажков выберите ресурсы, которые вы хотите импортировать.

   b. Если вы выбрали **Репозиторий** в качестве источника импорта, в открывшейся таблице выберите один или несколько пакетов репозитория.
7. Нажмите на кнопку **Импортировать**.
8. При необходимости устраните конфликты между импортированными из файла и существующими ресурсами.

При импорте шаблона отчета необходимо учитывать следующее:

- Если шаблон импортируется в любой тенант, то тенант импортируемого шаблона отчета указывается в качестве тенанта ресурса и тенанта источника данных.
- После импорта ресурсов необходимо указать пространства для виджетов с событиями и при необходимости расширить список тенантов.

Универсальность шаблона отчетов

Шаблон отчета в Kaspersky SIEM Cloud считается универсальным, если создается в тенанте Shared. Шаблоны отчетов, созданные в других тенантах, являются неуниверсальными.

Для работы с универсальным шаблоном отчета у пользователя должны быть следующие роли:

- Для создания, изменения параметров и удаления нужна роль Редактирование общих ресурсов. При наличии такой роли пользователь получает доступ ко всем общим ресурсам.

  Если роль пользователя предполагает работу с ресурсами КИИ, то признак КИИ может установить любой пользователь с ролью Редактирование общих ресурсов.

- Для просмотра списка универсальных шаблонов отчетов нужна роль Чтение общих ресурсов. При наличии таких прав пользователь получает доступ на чтение всех общих ресурсов.

Виджеты в универсальном шаблоне отчета отображаются с учетом следующего:

- Данные виджетов для тенантов отображаются в соответствии с доступом пользователя к тенантам, глобальным фильтром тенантов и конфигурацией шаблона отчетов или виджета.

- Данные виджетов при изменении параметров шаблона отчета можно посмотреть с помощью кнопки **Обновить предпросмотр**.

- Данные виджетов по событиям поступают из базы данных в соответствии с параметрами набора пространств пользователя. Если при формировании отчета оказывается, что у пользователя нет доступа к пространствам одного или нескольких тенантов, Kaspersky SIEM Cloud сформирует пустой отчет и отобразится сообщение о невозможности предоставления других результатов из-за отсутствия доступа к нужным пространствам.

- Данные виджетов в отчете могут формироваться с учетом КИИ или без учета КИИ. Для доступа к отчетам, в которых данные рассчитывались с учетом КИИ, у пользователя должна быть роль Доступ к КИИ.

- К универсальным отчетам применимы ограничения для виджетов активных листов и контекстных таблиц.

Сформированные отчеты

Все отчеты формируются с помощью шаблонов отчетов. Сформированные отчеты доступны на вкладке **Сформированные отчеты** в разделе **Мониторинг → Отчеты → Обнаружение и реагирование** и отображаются в таблице со следующей информацией:

- **Имя** – имя шаблона отчетов.

  Вы можете отсортировать шаблоны отчетов, нажав на значок сортировки ⌄ в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

  Вы также можете искать шаблоны отчетов по их названию, используя поле **Поиск**, расположенное над таблицей.

- **Период** – период времени, за который была извлечена аналитика отчета.

- **Последний отчет** – дата и время формирования последнего отчета.

- Вы можете отсортировать таблицу по этому столбцу, нажав на значок сортировки ⌄ в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

- **Тенант** – название тенанта, которому принадлежит отчет.
- **Пользователь** – имя пользователя, который сформировал отчет вручную. Если отчет был сформирован по расписанию, значение будет пустым.

При необходимости вы можете настроить отображение столбцов в таблице, нажав на значок шестеренки ⚙.

После выбора отчета в списке сформированных отчетов вы можете выполнить следующие действия с отчетами:

- Создать отчет.
- Открыть и просмотреть отчет.
- Сохранить сформированный отчет в нужном формате. Доступные форматы: HTML, PDF, CSV, разделенный CSV, Excel. По умолчанию во всех форматах выводится 250 строк. Максимальное количество строк, которые могут отображаться в таблицах в форматах PDF и HTML равно 500. Если вы хотите выводить в отчет более 500 строк, задайте в SQL-запросе желаемое значение параметра LIMIT и сохраните отчет в формате CSV.
- Настроить параметры шаблона отчета.
- Удалить отчет.

Просмотр отчетов

Чтобы просмотреть отчет:

1. В веб-консоли перейдите в раздел **Мониторинг → Отчеты → Обнаружение и реагирование → Сформированные отчеты**.
2. В таблице отчетов нажмите на название сформированного отчета.

   Откроется новая вкладка браузера с виджетами, отображающими аналитику отчетов. Если виджет отображает данные о событиях, алертах, инцидентах или активных листах, при нажатии на его заголовок открывается соответствующий раздел веб-консоли с активным фильтром и/или поисковым запросом, с помощью которых отображаются данные из виджета. К виджетам применяются значения по умолчанию.

   Если вы хотите просмотреть полные данные, выгрузите отчет в формате CSV с указанными параметрами из запроса.

   Если вы в настройке виджета включили переключатель **Итоговые значения**, на виджете отображается значение **Всего**, но при вложении или выгрузке отчета в форматах CSV и расширенный CSV значение **Всего** не отображается. Для отображения значения **Всего** в отчете, вы можете воспользоваться формулами Excel или переписать итоговое значение с виджета, или воспользоваться вложениями в формате PDF и HTML.
3. При необходимости сохраните отчет в выбранном формате с помощью кнопки **Сохранить как**.

Создание отчетов

Вы можете создать отчет вручную или настроить расписание, чтобы отчеты создавались автоматически.

Чтобы создать отчет вручную:

1. В веб-консоли перейдите в раздел **Мониторинг → Отчеты → Обнаружение и реагирование**.
2. Выполните одно из следующих действий:

   a. На вкладке **Сформированные отчеты** выполните следующие действия:

   - С помощью флажка выберите отчет в таблице со списком отчетов.
   - Нажмите на кнопку **Создать отчет**, расположенную над таблицей.

   b. На вкладке **Шаблоны**:

   - С помощью флажка выберите отчет в таблице со списком шаблонов отчета.
   - Нажмите на значок меню ⋮ и выберите в раскрывающемся списке **Запустить отчет**.

   В течение 15 секунд отчет будет создан и помещен на вкладку **Отчеты → Обнаружение и реагирование → Сформированные отчеты**.

Вы также можете настроить расписание отчетов для автоматического формирования отчетов.

Сохранение отчетов

Чтобы сохранить отчет в нужном формате:

1. В веб-консоли перейдите в раздел **Мониторинг → Отчеты → Обнаружение и реагирование → Сформированные отчеты**.
2. С помощью флажка выберите сформированный отчет в таблице со списком сформированных отчетов.
3. В раскрывающемся списке **Сохранить как**, расположенном над таблицей, выберите нужный формат: HTML, PDF, CSV, разделенный CSV, Excel.

   Отчет сохраняется в папку загрузки, настроенную в вашем браузере.

Отчет также можно сохранить в выбранном формате при просмотре.

Обновление отчетов

Чтобы обновить сформированный отчет:

1. В веб-консоли перейдите в раздел **Мониторинг → Отчеты → Обнаружение и реагирование → Сформированные отчеты**.
2. В таблице со списком сформированных отчетов выберите интересующий вас отчет.
3. Нажмите на кнопку **Создать отчет**, расположенную над таблицей.

   Отчет обновится в течение 15 секунд и будет доступен в разделе **Отчеты → Обнаружение и реагирование → Сформированные отчеты**.

Удаление отчетов

Чтобы удалить отчет:

1. В веб-консоли перейдите в раздел **Мониторинг → Отчеты → Обнаружение и реагирование → Сформированные отчеты**.
2. В таблице со списком сформированных отчетов выберите интересующий вас отчет.
3. Нажмите на кнопку **Удалить**, расположенную над таблицей.

   Откроется окно подтверждения.
4. Нажмите на кнопку **Удалить**.

   Выбранный отчет удален.

События и выборки событий

В этом разделе содержится информация о событиях и выборках событий, о типах событий, возникших в компонентах Kaspersky SIEM Cloud, и об управлении блокировкой частых событий.

О событиях в Kaspersky SIEM Cloud

Kaspersky SIEM Cloud позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования.

События по типу

В Kaspersky SIEM Cloud существуют следующие типы уведомлений:

- Общие события. Эти события возникают во всех управляемых приложениях "Лаборатории Касперского". Например, общее событие Вирусная атака. Общие события имеют строго определенные синтаксис и семантику. Общие события используются, например, в отчетах и панели мониторинга.
- Специфические события управляемых приложений "Лаборатории Касперского". Каждое управляемое приложение "Лаборатории Касперского" имеет собственный набор событий.

События по источнику

Просмотреть полный список событий, которые может генерировать приложение, можно на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть список событий в свойствах Сервера администрирования.

События могут генерироваться следующими приложениями:

- Компоненты приложения Kaspersky SIEM Cloud:
  - Сервер администрирования
  - Агент администрирования
- Управляемые приложения "Лаборатории Касперского"

  Подробнее о событиях, генерируемых управляемыми приложениями "Лаборатории Касперского", см. в документации соответствующего приложения.

События по уровню важности

Каждое событие имеет собственный уровень важности. В зависимости от условий возникновения, событию могут быть присвоены различные уровни важности. Существует четыре уровня важности событий:

- *Критическое событие* – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- *Отказ функционирования* – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы приложения или выполнения процедуры.
- *Предупреждение* – событие, не обязательно являющееся серьезным, однако указывающее на возможное возникновение проблемы в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа приложения может быть восстановлена без потери данных или функциональных возможностей.
- *Информационное сообщение* – событие, возникающее с целью информирования об успешном выполнении операции, корректной работе приложения или завершении процедуры.

Для каждого события задано время хранения, которое можно посмотреть или изменить в Kaspersky SIEM Cloud. Некоторые события не сохраняются в базе данных Сервера администрирования по умолчанию, поскольку для них установленное время хранения равно нулю. Во внешние системы можно экспортировать только те события, которые хранятся в базе данных Сервера администрирования не менее одного дня.

События компонентов Kaspersky SIEM Cloud

Каждый компонент Kaspersky SIEM Cloud имеет собственный набор типов событий. В этом разделе перечислены типы событий, которые происходят на Сервере администрирования и Агенте администрирования. Типы событий, которые возникают в приложениях "Лаборатории Касперского", в этом разделе не перечислены.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Структура данных описания типа события

Для каждого типа событий отображаются его имя, идентификатор, буквенный код, описание и время хранения по умолчанию.

- **Отображаемое имя типа события**. Этот текст отображается в Kaspersky SIEM Cloud, когда вы настраиваете события и при их возникновении.
- **Идентификатор типа события**. Этот цифровой код используется при обработке событий с использованием инструментов анализа событий сторонних производителей.
- **Тип события** (буквенный код). Этот код используется при просмотре и обработке событий с использованием публичных представлений базы данных Kaspersky SIEM Cloud и при экспорте событий в SIEM-системы.
- **Описание**. Этот текст содержит описание ситуации при возникновении события и описание того, что вы можете сделать в этом случае.
- **Срок хранения по умолчанию**. Это количество дней, в течение которых событие хранится в базе данных Сервера администрирования и отображается в списке событий Сервера администрирования. После окончания этого периода событие удаляется. Если значение времени хранения события указано 0, такие события регистрируются, но не отображаются в списке событий Сервера администрирования. Если вы настроили хранение таких событий в журнале событий операционной системы, вы можете найти их там.

  Можно изменить время хранения событий: Настройка срока хранения события.

События Сервера администрирования

В этом разделе содержится информация о событиях Сервера администрирования.

Критические события Сервера администрирования

В таблице ниже приведены события Сервера администрирования с уровнем важности **Критическое**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Срок действия сертификата Сервера администрирования для мобильных устройств истек	6129	KLSRV_EV_SRV_CERT_EXPIRED_DN	События этого типа возникают, если истек срок действия сертификатов Сервера администрирования для мобильных устройств и для устройств с защитой на уровне UEFI в сети. Вам необходимо обновить сертификат, срок действия которого истек.	180 дней
Аудит: Не удалось выполнить экспорт в SIEM-систему	5130	KLAUD_EV_SIEM_EXPORT_ERROR	События этого типа возникают при сбое экспорта событий в SIEM-систему из-за ошибки соединения с SIEM-системой.	180 дней
Устройство стало неуправляемым	4111	KLSRV_HOST_OUT_CONTROL	События этого типа возникают, если управляемое устройство видимо в сети, но не подключено к Серверу администрирования в течение заданного периода. Определите, что мешает правильной работе Агента администрирования на устройстве. Возможные причины могут включать проблемы сети и удаление Агента администрирования с устройства.	180 дней
Статус устройства "Критический"	4113	KLSRV_HOST_STATUS_CRITICAL	События этого типа возникают, если управляемому устройству назначен статус *Критический*. Вы можете настроить условия при выполнении которых, статус устройства изменяется на *Критический*.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Срок действия лицензии скоро истекает	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	События этого типа возникают, если приближается дата окончания срока действия коммерческой лицензии. Один раз в день Open Single Management Platform проверяет, не истек ли срок действия лицензии. События этого типа публикуются за 30 дней, 15 дней, 5 дней и 1 день, до истечения срока действия лицензии. Это количество дней невозможно изменить. Если Сервер администрирования выключен, в указанный день окончания срока действия лицензии, событие не будет опубликовано до следующего дня. После окончания срока действия коммерческой лицензии, Kaspersky SIEM Cloud работает в режиме Базовой функциональности. Вы можете ответить на событие следующими способами: • Убедитесь, что резервный лицензионный ключ добавлен на Сервер администрирования. • Если вы используете подписку, продлите ее. Неограниченная подписка продлевается автоматически, если предоплата поставщику услуг была своевременно внесена.	180 дней
Лицензионное ограничение превышено	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Один раз в день Kaspersky SIEM Cloud проверяет, не превышены ли лицензионные ограничения. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц, охватываемых лицензией. Даже если возникает это событие, клиентские устройства защищены. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются. • Предоставьте лицензию на большее количество устройств (добавьте действительный код активации или файл ключа на Сервер администрирования). Kaspersky SIEM Cloud определяет правила генерации событий при превышении лицензионного ограничения.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Режим ограниченной функциональности	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	События этого типа возникают, если Kaspersky SIEM Cloud начинает работать в режиме базовой функциональности, без поддержки Управления мобильными устройствами и Системного администрирования. Ниже приведены причины и соответствующие ответы на событие: • Срок действия лицензии истек. Предоставьте лицензию на полную функциональность Kaspersky SIEM Cloud (добавьте действительный код активации или файл ключа на Сервер администрирования). • Сервер администрирования управляет большим количеством устройств, чем может использоваться по предоставленной лицензии. Переместите устройства из состава групп администрирования одного Сервера в группы администрирования другого Сервера (если лицензионное ограничение другого Сервера не превышено).	180 дней
Срок действия MDM-сертификата истек	4132	KLSRV_CERTIFICATE_EXPIRED	События этого типа возникают, если истек срок действия клиентского сертификата на мобильных устройствах.	180 дней
Файл ключа добавлен в список запрещенных	4124	KLSRV_LICENSE_BLACKLISTED	События этого типа возникают, если "Лаборатория Касперского" добавила код активации или файл ключа, который вы используете, в список запрещенных. Обратитесь в Службу технической поддержки для получения подробной информации.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Обновления модулей приложений "Лаборатории Касперского" отозваны	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	События этого типа возникают, если обновления были отозваны техническими специалистами "Лаборатории Касперского", например, по причине их замены на более новые версии. Для таких обновлений отображается статус *Отозвано*. Событие не относится к патчам Kaspersky SIEM Cloud и не относится к модулям управляемых приложений "Лаборатории Касперского". Событие содержит причину, из-за которой обновления не установлены.	180 дней
Вирусная атака	• 26 (для компонента Защита от файловых угроз) • 27 (для компонента Защита от почтовых угроз) • 28 (для сетевого экрана)	GNRL_EV_VIRUS_OUTBREAK	События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения. Вы можете ответить на событие следующими способами: • Настройте пороговые значения в свойствах Сервера администрирования. • Создайте более строгую политику, которая будет активирована, или создайте задачу, которая будет запускаться при возникновении этого события.	

События отказа функционирования Сервера администрирования

В таблице ниже приведены события Сервера администрирования с уровнем важности **Отказ функционирования**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось выполнить копирование обновлений в заданную папку	4123	KLSRV_UPD_REPL_FAIL	События этого типа возникают, если обновления программного обеспечения копируются в общую папку (или папки). Вы можете ответить на событие следующими способами: • Проверить, имеет ли учетная запись пользователя, которая используется для получения доступа к папке (или папкам), права на запись. • Проверить, были ли изменены имя пользователя и/или пароль к папкам. • Проверить подключение к интернету, так как это может быть причиной события. Следуйте инструкциям по обновлению баз и модулей приложений.	180 дней
Не удалось выполнить опрос облачного сегмента	4143	KLSRV_KLCLOUD_SCAN_ERROR	События этого типа возникают, если Сервер администрирования не может опросить сегмент сети в облачном окружении. Прочтите информацию в описании события и отреагируйте соответствующим образом.	Не хранится
Для одной из групп лицензионных приложений превышено ограничение числа установок	4126	KLSRV_INVLICPROD_EXCEDED	Сервер администрирования генерирует события такого типа периодически (каждый час). События этого типа возникают, если в Kaspersky SIEM Cloud вы управляете лицензионными ключами приложений сторонних производителей и если количество установок превысило заданное в лицензионном ключе приложения стороннего производителя ограничение. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите приложение стороннего производителя с устройств, на которых оно не используется. • Используйте лицензию стороннего производителя на большее количество устройств. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений. В группу лицензионных приложений входят приложения сторонних производителей, отвечающие заданным вами критериям.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Нет свободного места на диске	4107	KLSRV_DISK_FULL	События этого типа возникают, если на жестком диске устройства, на котором установлен Сервер администрирования, заканчивается дисковое пространство. Освободите дисковое пространство на устройстве.	180 дней
Недостаточно места в базе данных Сервера администрирования	4110	KLSRV_DATABASE_FULL	События этого типа возникают, если нет свободного места в базе Сервера администрирования. Сервер администрирования не работает, если его база данных переполнена и дальнейшая запись в базу данных невозможна. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие: • Ограничьте количество событий, хранящихся в базе данных Сервера администрирования. • В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль приложений. Вы можете изменить параметры политики Kaspersky Endpoint Security, касающиеся хранения событий компонента Контроль приложений в базе данных Сервера администрирования. Просмотрите информацию о выборе СУБД.	180 дней
Ошибка времени выполнения	4125	KLSRV_RUNTIME_ERROR	События этого типа возникают из-за неизвестных проблем. Чаще всего это проблемы СУБД, проблемы с сетью и другие проблемы с программным и аппаратным обеспечением. Подробную информацию о событии можно найти в его описании.	180 дней
Общая папка недоступна	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	События этого типа возникают, если общая папка Сервера администрирования недоступна. Вы можете ответить на событие следующими способами: • Убедитесь, что Сервер администрирования (на котором находится общая папка) включен и доступен. • Проверьте, были ли изменены имя пользователя и/или пароль к папке. • Проверьте подключение к сети.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
База данных Сервера администрирования недоступна	4109	KLSRV_DATABASE_UNAVAILABLE	События этого типа возникают, если база Сервера администрирования становится недоступной. Вы можете ответить на событие следующими способами: • Проверьте, доступен ли удаленный сервер, на котором установлена СУБД. • Просмотрите журналы событий СУБД и найдите причину недоступности базы Сервера администрирования.	180 дней

События предупреждения Сервера администрирования

В таблице ниже приведены события Сервера администрирования с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

События предупреждения Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Срок действия сертификата Сервера администрирования для мобильных устройств истекает	6128	KLSRV_EV_SRV_CERT_EXPIRES_SOON	События этого типа возникают, если истек срок действия сертификатов Сервера администрирования для мобильных устройств и для устройств с защитой на уровне UEFI в сети. Вам необходимо обновить сертификат, срок действия которого истек.	90 дней
Срок действия APNs-сертификата истекает	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	События этого типа возникают, если до истечения срока действия APNs-сертификата остается менее 14 дней. При истечении срока действия APNs-сертификата, вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM. Рекомендуется запланировать обновление APNs-сертификата до истечения срока его действия.	Не хранится
Срок действия APNs-сертификата истек	4135	KLSRV_APN_CERTIFICATE_EXPIRED	События этого типа происходят, если истекает срок действия APNs-сертификата. Вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM.	Не хранится

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Аудит: Не удалось выполнить тестовое подключение к SIEM-серверу	5120	KLAUD_EV_SIEM_TEST_FAILED	События этого типа возникают при сбое автоматической проверки подключения к SIEM-серверу.	90 дней
Сертификат удален	4134	KLSRV_CERTIFICATE_REMOVED	События этого типа возникают, если администратор удаляет сертификат любого типа (общий, почтовый, VPN) для Управления мобильными устройствами. После удаления сертификата мобильные устройства, подключенные по этому сертификату, не смогут подключиться к Серверу администрирования. Это событие может быть полезно при исследовании неисправностей, связанных с Управлением мобильными устройствами.	90 дней
Сертификат запрошен	4133	KLSRV_CERTIFICATE_REQUESTED	События этого типа возникают, если не удается автоматически перевыпустить сертификат для Управления мобильными устройствами. Ниже приведены возможные причины событий и соответствующие действия по реагированию на событие: • Автоматический перевыпуск был инициирован для сертификата, для которого параметр **Автоматически перевыпускать сертификат, если это возможно**. Это могло произойти из-за ошибки, которая возникла при создании сертификата. Может потребоваться перевыпуск сертификата вручную. • Если вы используете интеграцию с инфраструктурой открытых ключей, причиной может быть отсутствие атрибута SAM-Account-Name учетной записи, которая используется для интеграции с PKI и для выпуска сертификата. Просмотрите свойства учетной записи.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Конфликт имен устройств	4102	KLSRV_EVENT_HOSTS_CONFLICT	События этого типа возникают, если Сервер администрирования рассматривает два или более управляемых устройства как одно устройство. Чаще всего это происходит, когда клонированный жесткий диск использовался для развертывания приложений на управляемых устройствах и без переключения Агента администрирования в режим клонирования выделенного диска на эталонном устройстве. Чтобы избежать этой проблемы, перед клонированием жесткого диска этого устройства переключите Агент администрирования в режим клонирования диска на эталонном устройстве.	90 дней
Разорвано соединение с главным Сервером администрирования	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с главным Сервером администрирования. Прочтите журнал событий операционной системы на устройстве, на котором установлен главный Сервер администрирования, и отреагируйте соответствующим образом.	90 дней
Разорвано соединение с подчиненным Сервером администрирования	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с подчиненным Сервером администрирования. Прочтите журнал событий операционной системы на устройстве, на котором установлен подчиненный Сервер администрирования, и отреагируйте соответствующим образом.	90 дней
Устройство долго не проявляет активности в сети	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	События этого типа возникают, если управляемое устройство неактивно в течение некоторого времени. Чаще всего это происходит, когда управляемое устройство выводится из эксплуатации. Вы можете ответить на событие следующими способами: • Удалите устройство из списка управляемых устройств вручную. Укажите интервал, по истечении которого создается событие **Устройство долго не проявляет активности в сети** с помощью OSMP Console. • Укажите интервал, по истечении которого устройство автоматически удаляется из группы с помощью OSMP Console.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Статус устройства "Предупреждение"	4114	KLSRV_HOST_STATUS_WARNING	События этого типа возникают, если управляемому устройству назначен статус *Предупреждение*. Вы можете настроить условия при выполнении которых, статус устройства изменяется на *Предупреждение*.	90 дней
Не удалось скачать файл на устройство	4165	KLSRV_FILE_DOWNLOAD_FAILED	События этого типа возникают в следующих случаях: • Вы пытаетесь загрузить файл в корпоративный контейнер, но корпоративный контейнер не был создан. • На устройстве недостаточно места. • Не удалось скачать информацию о файле с сервера. • Не удалось скачать содержимое файла с сервера. • Не удалось создать папку на устройстве. • На личном устройстве отсутствует доступ к файлам. • В корпоративном контейнере отсутствует доступ к файлу.	90 дней
Не удалось отправить FCM-сообщение на FCM-сервер	4140	KLSRV_GCM_GENERAL_ERROR	События этого типа возникают из-за непредвиденных ошибок на стороне Сервера администрирования при работе с HTTP-протоколом Google Firebase Cloud Messaging. Прочтите информацию в описании события и отреагируйте соответствующим образом. Если вы не можете найти решение проблемы самостоятельно, рекомендуем вам обратиться в Службу технической поддержки "Лаборатории Касперского".	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось отправить FCM-сообщение на мобильное устройство	4138	KLSRV_GCM_DEVICE_ERROR	События этого типа возникают, если Управление мобильными устройствами настроено на использование Google Firebase Cloud Messaging (FCM) для подключения к управляемым мобильным устройствам с операционной системой Android, а FCM-сервер не может обработать некоторые запросы, полученные от Сервера администрирования. Это означает, что некоторые управляемые мобильные устройства не будут получать push-уведомление. Прочтите HTTP код в описании события и ответьте соответствующим образом. Дополнительная информация о HTTP кодах, полученных от FCM-сервера, и связанных с ними ошибках есть в документации службы Google Firebase (см. главу "Downstream message error response codes").	90 дней
Обнаружено получение частных событий		KLSRV_EVENT_SPAM_EVENTS_DETECTED	События этого типа возникают, если Сервер администрирования регистрирует частые события на управляемом устройстве. Дополнительную информацию см. в следующих разделах: Блокировка частых событий.	90 дней
Жесткий диск почти заполнен	4105	KLSRV_NO_SPACE_ON_VOLUMES	События этого типа возникают, если на устройстве, на котором установлен Сервер администрирования, почти закончилось дисковое пространство. Освободите дисковое пространство на устройстве.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
HTTP-ошибка при отправке FCM-сообщения на FCM-сервер	4139	KLSRV_GCM_HTTP_ERROR	События этого типа возникают, если Управление мобильными устройствами настроено на использование Google Firebase Cloud Messaging (FCM) для подключения управляемых мобильных устройств с операционной системой Android, а FCM-сервер возвращает запрос Серверу администрирования с кодом HTTP, отличным от 200 (OK). Ниже приведены возможные причины событий и соответствующие действия по реагированию на событие: • Проблемы на стороне FCM-сервера. Прочтите HTTP код в описании события и ответьте соответствующим образом. Дополнительная информация о HTTP кодах, полученных от FCM-сервера, и связанных с ними ошибках есть в документации службы Google Firebase (см. главу "Downstream message error response codes"). • Проблемы на стороне прокси-сервера (если вы используете прокси-сервер). Прочтите HTTP код в описании события и ответьте соответствующим образом.	90 дней
Лицензионное ограничение превышено	4098	KLSRV_EV_LICENSE_CHECK_100_110	Один раз в день Kaspersky SIEM Cloud проверяет, не превышены ли лицензионные ограничения. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии составляет от 100% до 110% от общего количества единиц, охватываемых лицензией. Даже если возникает это событие, клиентские устройства защищены. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются. • Предоставьте лицензию на большее количество устройств (добавьте действительный код активации или файл ключа на Сервер администрирования). Kaspersky SIEM Cloud определяет правила генерации событий при превышении лицензионного ограничения.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Для одной из групп лицензионных приложений скоро будет достигнуто ограничение числа установок	4128	KLSRV_INVLICPROD_EXPIRED_SOON	События этого типа возникают, когда истекает срок действия одного из лицензионных ключей сторонних приложений, входящих в группу лицензионных приложений. В результате число разрешенных установок для одной из групп будет уменьшено. Вы можете ответить на событие следующими способами: • Если приложение стороннего производителя не используется на каких-то управляемых устройствах, удалите приложение с этих устройств. • Если вы ожидаете, что количество установок для приложения стороннего производителя превысит разрешенное ограничение в ближайшем будущем, рассмотрите возможность получения лицензии приложения стороннего производителя на большее количество устройств заранее. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений.	90 дней
Зарегистрированы новые обновления модулей приложений "Лаборатории Касперского"	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	События этого типа возникают, если Сервер администрирования регистрирует новые обновления приложений "Лаборатории Касперского", установленных на управляемых устройствах, для установки которых требуется одобрение. Одобрите или отклоните обновления с помощью Web Console.	90 дней
Недостаточно места в базе данных Сервера администрирования	4106	KLSRV_NO_SPACE_IN_DATABASE	События этого типа возникают, если свободное место в базе Сервера администрирования ограничено. Если вы не устраните эту проблему, скоро база данных Сервера администрирования достигнет своей емкости и Сервер администрирования не будет работать. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие. • Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования. Просмотрите информацию о выборе СУБД.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Превышено ограничение числа событий, началось удаление событий из базы данных	4145	KLSRV_EVP_DB_TRUNCATING	События такого типа возникают, если удаление старых событий из базы данных Сервера администрирования началось после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования. Вы можете ответить на событие следующими способами: • Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования.	Не хранится
Превышено ограничение числа событий, удалены события из базы данных	4146	KLSRV_EVP_DB_TRUNCATED	События такого типа возникают, если старые события удалены из базы данных Сервера администрирования после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования. Вы можете ответить на событие следующими способами: • Укажите максимально допустимое количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования.	Не хранится

Информационные события Сервера администрирования

В таблице ниже приведены события Сервера администрирования с уровнем важности **Информационное сообщение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Информационные события Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Срок действия сертификата Сервера администрирования для мобильных устройств обновлен	6127	KLSRV_EV_SRV_CERT_RENEWED	События этого типа возникают, если сертификат Сервера администрирования был обновлен.	30 дней
Аудит: Подключение к Серверу администрирования было прервано	4151	KLAUD_EV_SERVERDISCONNECT		30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Аудит: Подключение к Серверу администрирования	4147	KLAUD_EV_SERVERCONNECT	События этого типа возникают при подключении пользователя к Серверу администрирования с помощью OSMP Console. Такие события включают информацию об IP-адресе устройства, на котором установлен Сервер OSMP Console.	30 дней
Аудит: Ключи шифрования импортированы/ экспортированы	5100	KLAUD_EV_DPEKEYSEXPORT	Например, это событие происходит во время переноса данных.	30 дней
Аудит: Изменение параметров группы	4149	KLAUD_EV_ADMGROUP_CHANGED	События этого типа возникают при изменении группы безопасности.	30 дней
Аудит: Изменение объекта	4148	KLAUD_EV_OBJECTMODIFY	Это событие отслеживает изменения в следующих объектах: • группах администрирования; • группах безопасности; • пользователях; • управляемых устройствах; • инсталляционных пакетах; • задачах; • политиках; • Серверах; • виртуальных Серверах.	30 дней
Аудит: Свойства объекта были изменены	4152	KLAUD_EV_OBJECTPROPMODIFIED	Это событие отслеживает изменения в следующих параметрах: • пользователь; • лицензия; • Сервер; • виртуальный Сервер.	30 дней
Аудит: Изменение статуса объекта	4150	KLAUD_EV_TASK_STATE_CHANGED	Например, это событие возникает, если задача завершилась ошибкой.	30 дней
Аудит: Тестовое подключение к SIEM-серверу выполнено успешно	5110	KLAUD_EV_SIEM_TEST_SUCCESS	События этого типа возникают при успешном подключении к SIEM-серверу.	30 дней
Аудит: Права пользователя были изменены	4153	KLAUD_EV_OBJECTACLMODIFIED	События этого типа возникают, если права пользователя были изменены.	30 дней
Установлено соединение с главным Сервером администрирования	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Установлено соединение с подчиненным Сервером администрирования	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	Подробнее см. в статье Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования.	30 дней
Базы обновлены	4144	KLSRV_UPD_BASES_UPDATED	События этого типа возникают, когда задача **Загрузка обновлений в хранилище Сервера администрирования** завершает обновление базы данных.	30 дней
Устройство было автоматически перемещено с помощью правила	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	События этого типа возникают, если устройства были перемещены в группы администрирования в соответствии с правилами перемещения устройств. Для каждого перемещенного устройства публикуется отдельное событие.	30 дней
Устройство удалено из группы: долгое отсутствие активности в сети	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	События этого типа возникают, когда устройства были автоматически удалены из группы из-за неактивности.	30 дней
Идентификатор экземпляра FCM мобильного устройства изменен	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	События этого типа возникают при изменении токена Firebase Cloud Messaging на устройстве. Информацию о ротации токенов FCM см. в документации сервиса Firebase.	30 дней
Файл загружен на Сервер администрирования	4162	KLSRV_FILE_UPLOADED	События этого типа возникают, если администратор загрузил файл в список в Web Console: **Управление активами → Мобильные → Приложения и файлы → Файлы**.	30 дней
Файл удален с Сервера администрирования	4163	KLSRV_FILE_REMOVED	События этого типа возникают, если администратор удалил файл из списка в Web Console: **Управление активами → Мобильные → Приложения и файлы → Файлы**.	30 дней
Файл загружен на устройство	4164	KLSRV_FILE_DOWNLOADED	События этого типа возникают в следующих случаях: • Администратор загрузил файл на свое рабочее место из списка в Web Console: **Управление активами → Мобильные → Приложения и файлы → Файлы**. • Файл из списка **Управление активами → Мобильные → Приложения и файлы → Файлы** загружен на устройство, на котором установлено приложение Kaspersky Endpoint Security для Android.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось загрузить файл на устройство	4165	KLSRV_FILE_DOWNLOAD_FAILED	События этого типа возникают в следующих случаях: • Произошла ошибка при попытке администратора загрузить файл на свое рабочее место из списка в Web Console: **Управление активами** → **Мобильные** → **Приложения и файлы** → **Файлы**. • Произошла ошибка при загрузке файла из списка **Управление активами** → **Мобильные** → **Приложения и файлы** → **Файлы** на устройство, на котором установлено приложение Kaspersky Endpoint Security для Android.	30 дней
Появились файлы для отправки на анализ в "Лабораторию Касперского"	4131	KLSRV_APS_FILE_APPEARED		30 дней
Для одной из групп лицензионных приложений число разрешенных установок исчерпано более чем на 90%	4127	KLSRV_INVLICPROD_FILLED	События этого типа возникают, если количество установок приложений сторонних производителей, включенных в группу лицензионных приложений, достигает 90% от максимально допустимого значения, указанного в свойствах лицензионного ключа. Вы можете ответить на событие следующими способами: • Если приложение стороннего производителя не используется на каких-то управляемых устройствах, удалите приложение с этих устройств. • Если вы ожидаете, что количество установок для приложения стороннего производителя превысит разрешенное ограничение в ближайшем будущем, рассмотрите возможность получения лицензии приложения стороннего производителя на большее количество устройств заранее. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений.	30 дней
Обнаружено новое устройство	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	События этого типа возникают при обнаружении новых сетевых устройств.	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Лицензионный ключ использован более чем на 90%	4097	KLSRV_EV_LICENSE_CHECK_90	События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии превышает 90% от общего количества лицензионных единиц, охватываемых лицензией. Даже при превышении лицензионных ограничений клиентские устройства защищены. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются. • Предоставьте лицензию на большее количество устройств (добавьте действительный код активации или файл ключа на Сервер администрирования). Kaspersky SIEM Cloud определяет правила генерации событий при превышении лицензионного ограничения.	30 дней
Резервный сертификат Сервера администрирования для мобильных устройств создан	6126	KLSRV_EV_SRV_CERT_RESERVE_CREATED	События этого типа возникают, если сертификат Сервера администрирования создан.	30 дней
Обновления успешно скопированы в заданную папку	4122	KLSRV_UPD_REPL_OK	События этого типа возникают, когда задача **Загрузка обновлений в хранилище Сервера администрирования** завершает копирование файлов в указанную папку.	30 дней

События **Резервный сертификат создан** и **Сертификат обновлен** автоматически публикуются Сервером администрирования и отображаются в Консоли администрирования только при выполнении соответствующих этим событиям операций для сертификатов Сервера администрирования для мобильных устройств и устройств с защитой на уровне UEFI.

События Агента администрирования

В этом разделе содержится информация о событиях Агента администрирования.

События предупреждения Агента администрирования

В таблице ниже приведены события Агента администрирования с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

События предупреждения Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Прокси-сервер KSN был запущен. Не удалось проверить доступность KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	События этого типа возникают при сбое тестового соединения для настроенного подключения прокси-сервера KSN.	30 дней
Произошла проблема безопасности	549	GNRL_EV_APP_INCIDENT_OCCURED	События этого типа возникают при обнаружении инцидента на устройстве. Например, это событие возникает, когда на устройстве мало места на диске.	30 дней
Обнаружен файл sudoers, который не соответствует референсному значению	7724	KLNAG_EV_SUDOER_DIFFERENT	События этого типа возникают, если есть несовпадение между файлом sudoers и референсным файлом.	30 дней
Установка обновления стороннего программного обеспечения отложена	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	Например, события этого типа возникают, когда отклоняется Лицензионное соглашение для установки обновлений приложений сторонних производителей.	30 дней
Установка обновления стороннего ПО завершена с предупреждением	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	Скачайте файлы трассировки и проверьте значение поля KLRI_PATCH_RES_DESC.	30 дней
Управление учетными записями: предупреждения	7722	KLNAG_EV_USR_MNG_WRN	Общее событие предупреждения.	30 дней
Возвращено предупреждение во время установки обновления модулей приложений	7701	KLNAG_EV_PATCH_INSTALL_WARNING	Скачайте файлы трассировки и проверьте значение поля KLRI_PATCH_RES_DESC.	30 дней

Информационные события Агента администрирования

В таблице ниже приведены события Агента администрирования с уровнем критичности **Информационное сообщение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Информационные события Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Установлено приложение	7703	KLNAG_EV_INV_APP_INSTALLED	30 дней
Приложение удалено	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 дней
Получен сертификат для HTTPS-порта Веб-сервера	—	WEB_SERVER_CERTIFICATE_RENEWED	30 дней
Устройство авторизовано	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Обнаружено новое устройство	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 дней
Устройство удалено	7709	KLNAG_EV_DEVICE_REMOVE	30 дней
Запущена установка обновления модулей приложений	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 дней
Прокси-сервер KSN был запущен. Проверка доступности KSN прошла успешно	7719	KSNPROXY_STARTED_CON_CHK_OK	30 дней
Прокси-сервер KSN остановлен	7720	KSNPROXY_STOPPED	30 дней
Установлено наблюдаемое приложение	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 дней
Удалено наблюдаемое приложение	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 дней
Новое устройство добавлено	7708	KLNAG_EV_DEVICE_ARRIVAL	30 дней
Корневой сертификат установлен	7727	KLNAG_EV_ROOT_CERT_INSTALLED	30 дней
Корневые сертификаты удалены	7729	KLNAG_EV_ROOT_CERT_REMOVED	30 дней
Файл sudoers успешно восстановлен до референсного значения	7725	KLNAG_EV_SUDOER_RESTORED	30 дней
Установлено стороннее приложение	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 дней
Обновление для приложений стороннего производителя установлено успешно	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 дней
Запущена установка обновления стороннего ПО	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 дней
Обновление модулей приложений успешно установлено	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 дней
Управление учетными записями: информационные сообщения	7721	KLNAG_EV_USR_MNG_INF	30 дней
Веб-Сервер запущен на устройстве	—	WEB_SERVER_STARTED	30 дней
Веб-Сервер остановлен на устройстве	—	WEB_SERVER_STOPPED	30 дней
Совместный доступ к рабочему столу Windows: приложение было запущено	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 дней
Совместный доступ к рабочему столу Windows: файл был изменен	7713	KLUSRLOG_EV_FILE_MODIFIED	30 дней
Совместный доступ к рабочему столу Windows: файл был прочитан	7712	KLUSRLOG_EV_FILE_READ	30 дней
Совместный доступ к рабочему столу Windows: предоставлен	7715	KLUSRLOG_EV_WDS_BEGIN	30 дней
Совместный доступ к рабочему столу Windows: завершен	7716	KLUSRLOG_EV_WDS_END	30 дней

События отказа функционирования Агента администрирования

В таблице ниже приведены события Агента администрирования Kaspersky SIEM Cloud с уровнем важности **Отказ функционирования**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось установить корневые сертификаты	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	Событие содержит описание ошибки установки сертификатов.	30 дней
Не удалось установить обновление стороннего производителя	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	События этого типа возникают, если используются возможности Системного администрирования, и если обновление программного обеспечения сторонних производителей прошло неуспешно. Проверьте, корректна ли ссылка на приложение стороннего производителя. Прочтите описание события.	30 дней
Не удалось установить обновления Windows	7717	KLNAG_EV_WUA_INSTALL_ERROR	События этого типа возникают, если обновления Центра обновления Windows были неуспешными. Прочтите описание события. Поищите описание ошибки в базе знаний Microsoft. Обратитесь в службу технической поддержки Microsoft, если вы не можете решить проблему самостоятельно.	30 дней
Не удалось удалить корневые сертификаты	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	Событие содержит описание ошибки удаления сертификатов.	30 дней
Не удалось восстановить файл sudoers до референсного значения	7726	KLNAG_EV_SUDOER_RESTORED_ERR	Событие содержит описание ошибки замены файла sudoers.	30 дней
Ошибка при установке обновления	7702	KLNAG_EV_PATCH_INSTALL_ERROR	События этого типа возникают, если автоматическая установка обновлений и патчей для компонентов Kaspersky SIEM Cloud прошла неуспешно. Событие не относится к обновлениям управляемых приложений "Лаборатории Касперского". Прочтите описание события. Причиной этого события может быть проблема операционной системы Windows на Сервере администрирования. Если в описании упоминается какая-либо проблема конфигурации Windows, устраните эту проблему.	30 дней
Управление учетными записями: ошибки	7723	KLNAG_EV_USR_MNG_ERR	Общее событие предупреждения.	30 дней

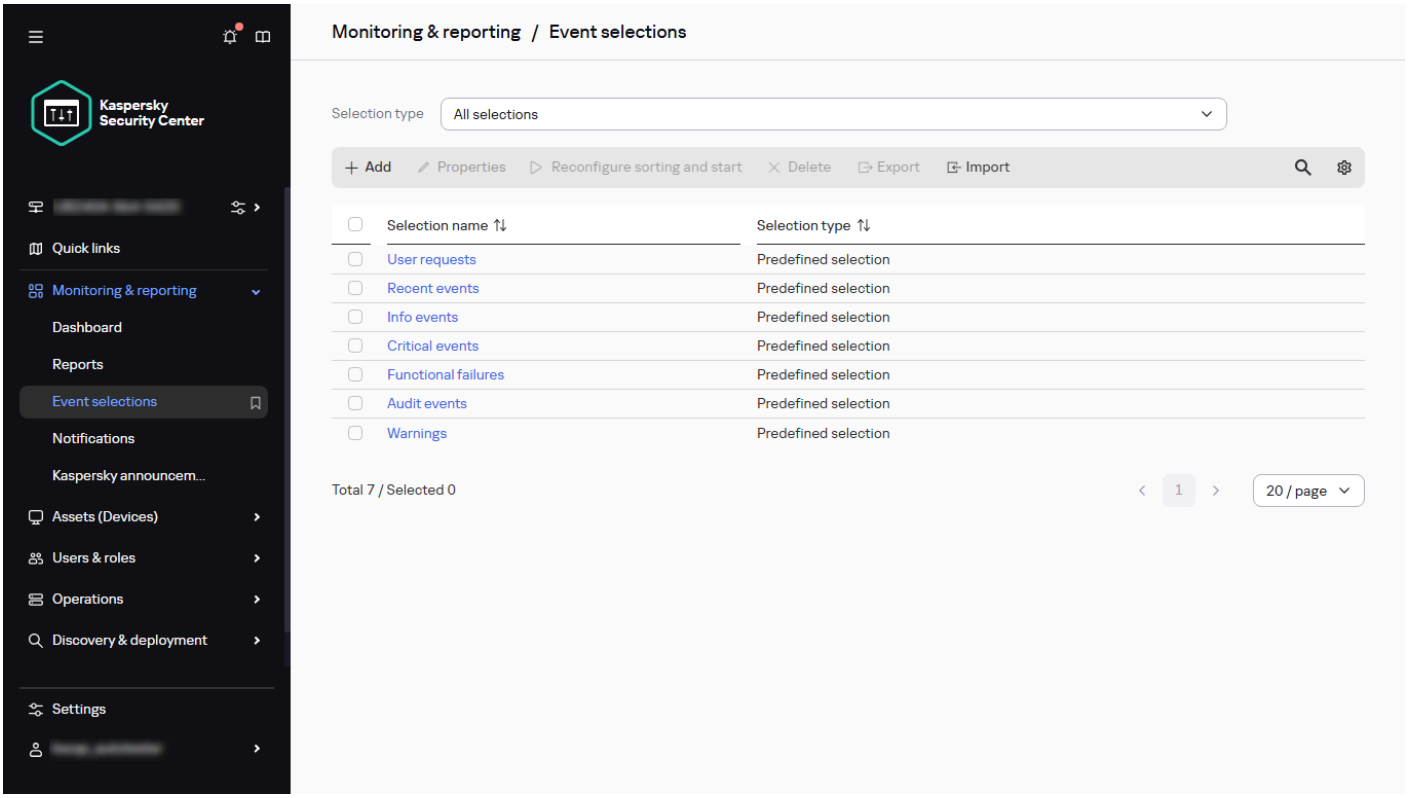
Использование выборок событий

Выборки событий предназначены для просмотра на экране именованных наборов событий, которые выбраны из базы данных Сервера администрирования. Эти типы событий сгруппированы по следующим категориям:

- Уровень важности: **Критические события**, **Отказы функционирования**, **Предупреждения** и **Информационные события**.
- Время: **Последние события**.
- Тип: **Запросы пользователей** и **События аудита**.

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе OSMP Console.

Выборки событий доступны в OSMP Console в разделе **Мониторинг → Выборки событий**.



Список выборок событий

По умолчанию выборки событий включают информацию за последние семь дней.

Kaspersky SIEM Cloud имеет набор выборок (предопределенных) по умолчанию:

- События с разным уровнем важности:
  - **Критические события.**
  - **Отказ функционирования.**

    - **Предупреждения.**
    - **Информационные события.**
- **Запросы пользователей** (события управляемых приложений).
- **Последние события** (за последнюю неделю).
- **События аудита**.

Вы можете также создавать и настраивать дополнительные пользовательские выборки событий. В пользовательских выборках вы можете фильтровать события по свойствам устройств, в которых они возникли (по именам устройств, IP-диапазонам и группам администрирования), по типам событий и уровням важности, по названию приложения и компонента, а также по временному интервалу. Также можно включить результаты задачи в область поиска. Вы также можете использовать поле поиска, в котором можно ввести слово или несколько слов. Отображаются все события, содержащие любые введенные слова в любом месте их свойств (таких как имя события, описание, имя компонента).

Как для предопределенных выборок, так и для пользовательских выборок вы можете ограничить количество отображаемых событий или количество записей для поиска. Оба варианта влияют на время, за которое Kaspersky SIEM Cloud отображает события. Чем больше база данных, тем более трудоемким может быть процесс.

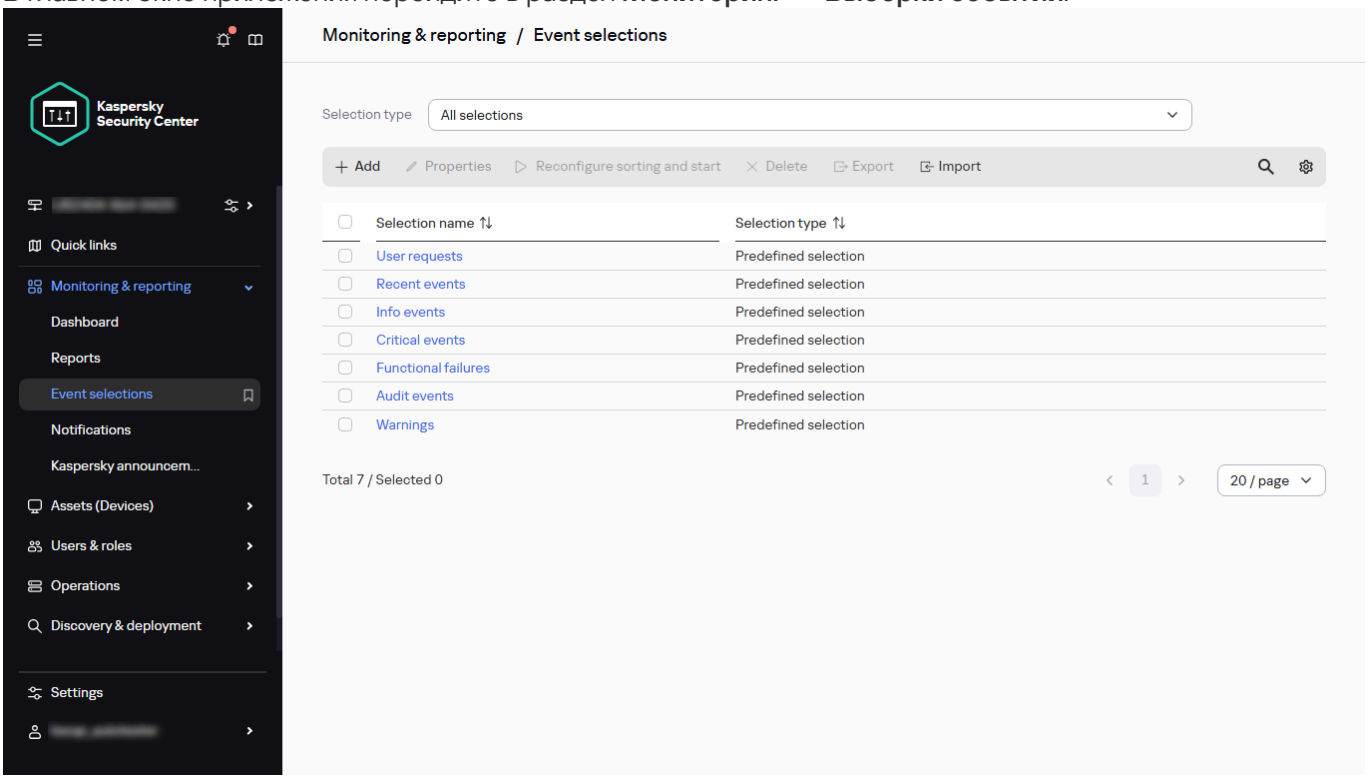
Вы можете выполнить следующее:

- Изменить параметры выборки событий.
- Сгенерировать выборки событий.
- Просмотреть сведения о выбранных выборках событий.
- Удалить выборки событий.
- Удалить события из базы данных Сервера администрирования.

Создание выборки событий

Чтобы создать выборку событий:

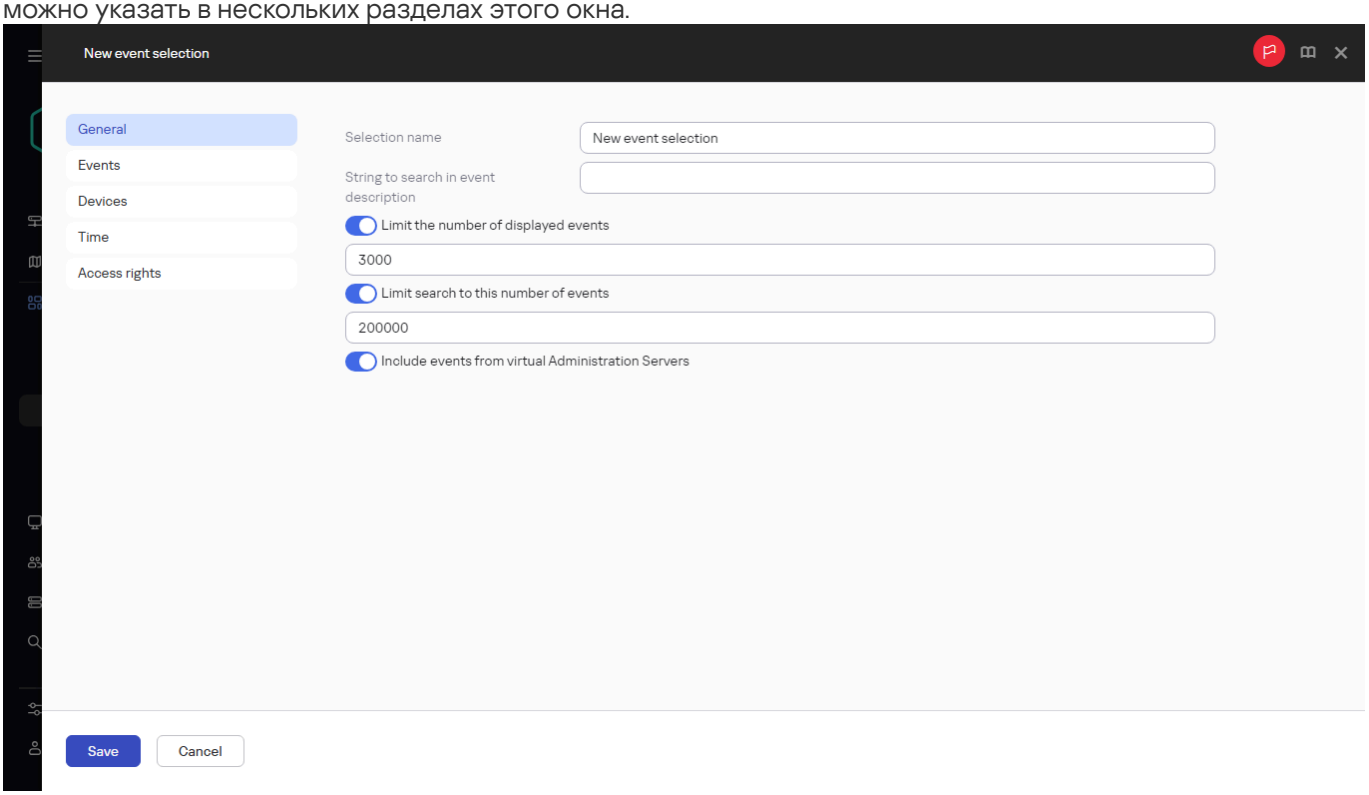
1. В главном окне приложения перейдите в раздел **Мониторинг → Выборки событий**.



Список выборок событий

2. Нажмите на кнопку **Добавить**.

3. В открывшемся окне **Новая выборка событий** укажите параметры новой выборки событий. Параметры можно указать в нескольких разделах этого окна.



Создание выборки событий.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   Откроется окно подтверждения.

5. Чтобы просмотреть результат выборки событий, установите флажок **Перейти к результатам выборки**.

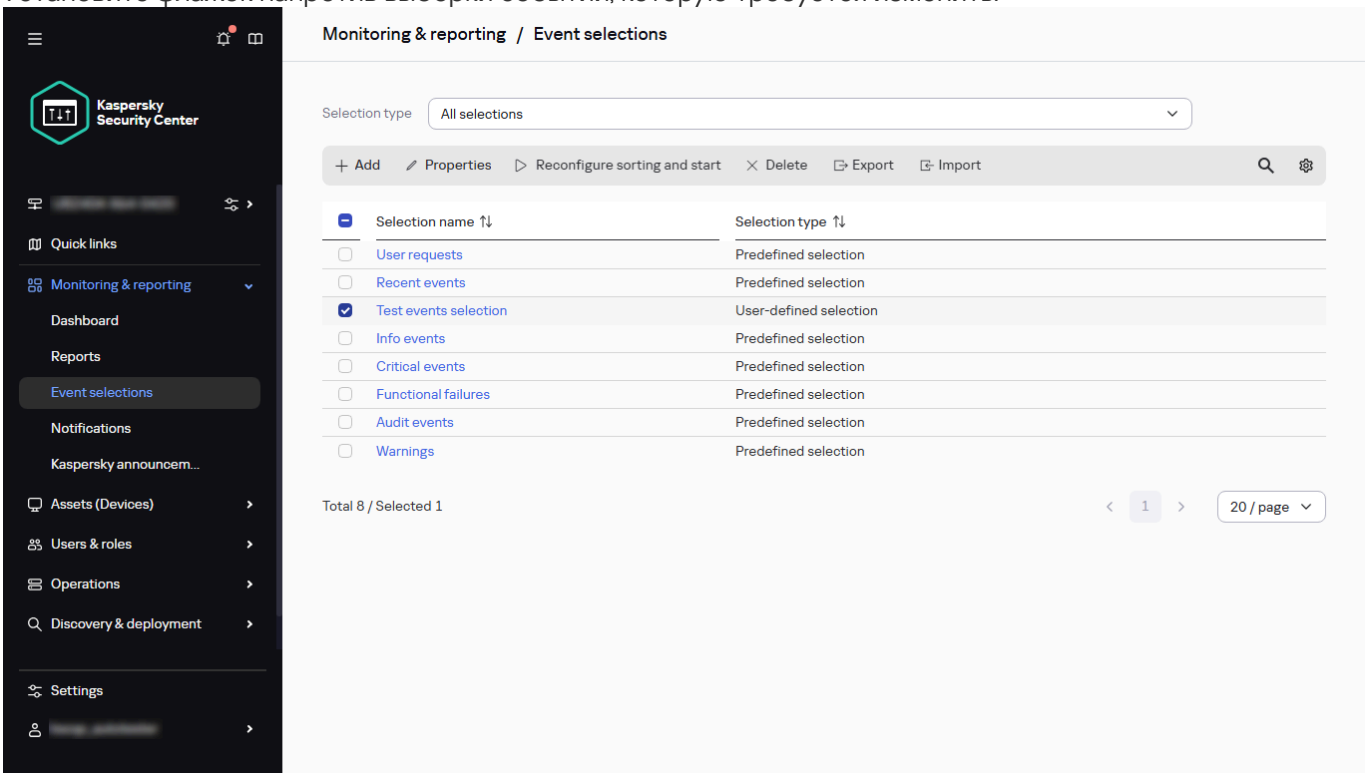
6. Нажмите на кнопку **Сохранить**, чтобы подтвердить создание выборки событий.

Если был установлен флажок **Перейти к результатам выборки**, результат выборки событий будет отображен на экране. В противном случае новая выборка событий появится в списке выборок событий.

Изменение выборки событий

Чтобы изменить выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется изменить.



Список выборок событий

3. Нажмите на кнопку **Свойства**.

   Откроется окно свойств выборки событий.

4. Отредактируйте свойства выборки событий.

   > Для стандартной выборки событий можно редактировать свойства только на следующих вкладках: **Общие** (за исключением имени выборки), **Время** и **Права доступа**.

   Для пользовательских выборок можно изменять все свойства.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

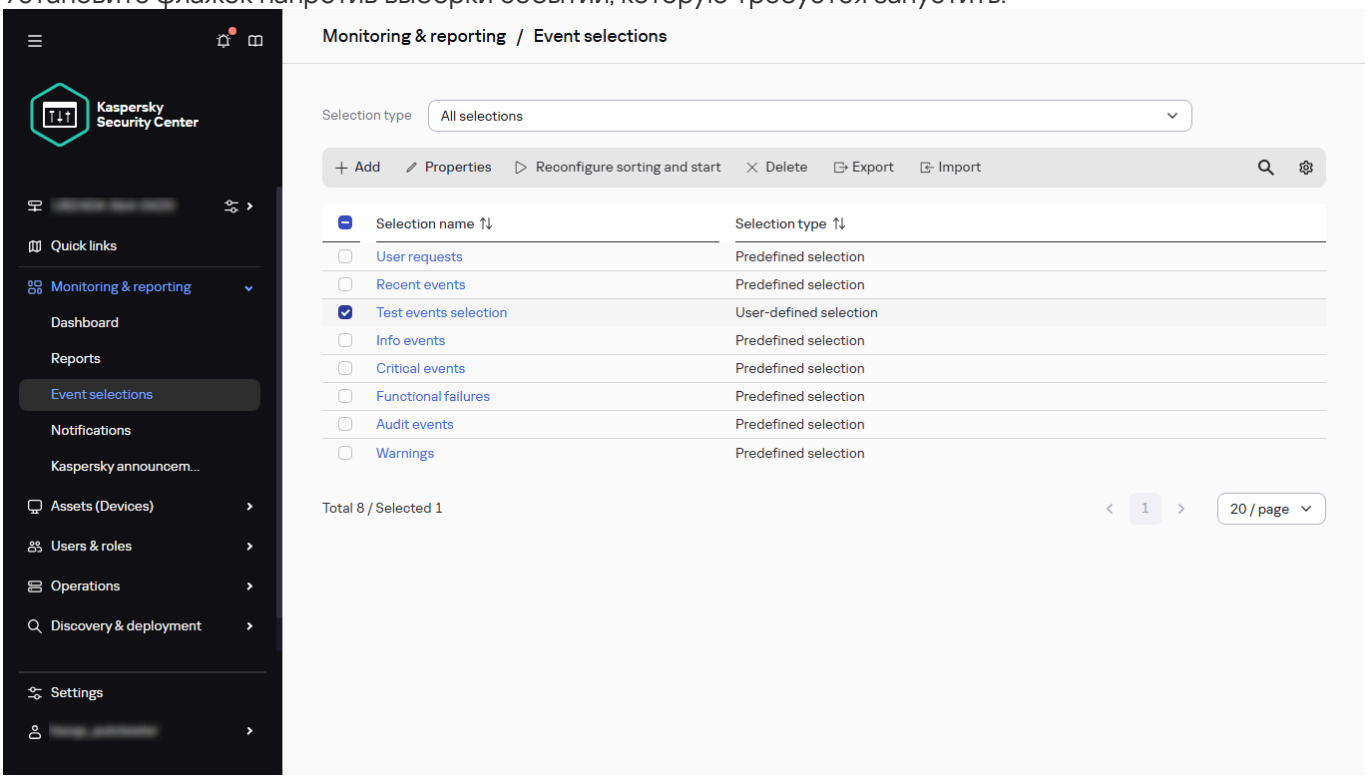
Измененная выборка событий отображается в списке.

Просмотр списка выборки событий

Просмотр выборки событий:

1. В главном окне приложения перейдите в раздел **Мониторинг → Выборки событий**.

2. Установите флажок напротив выборки событий, которую требуется запустить.



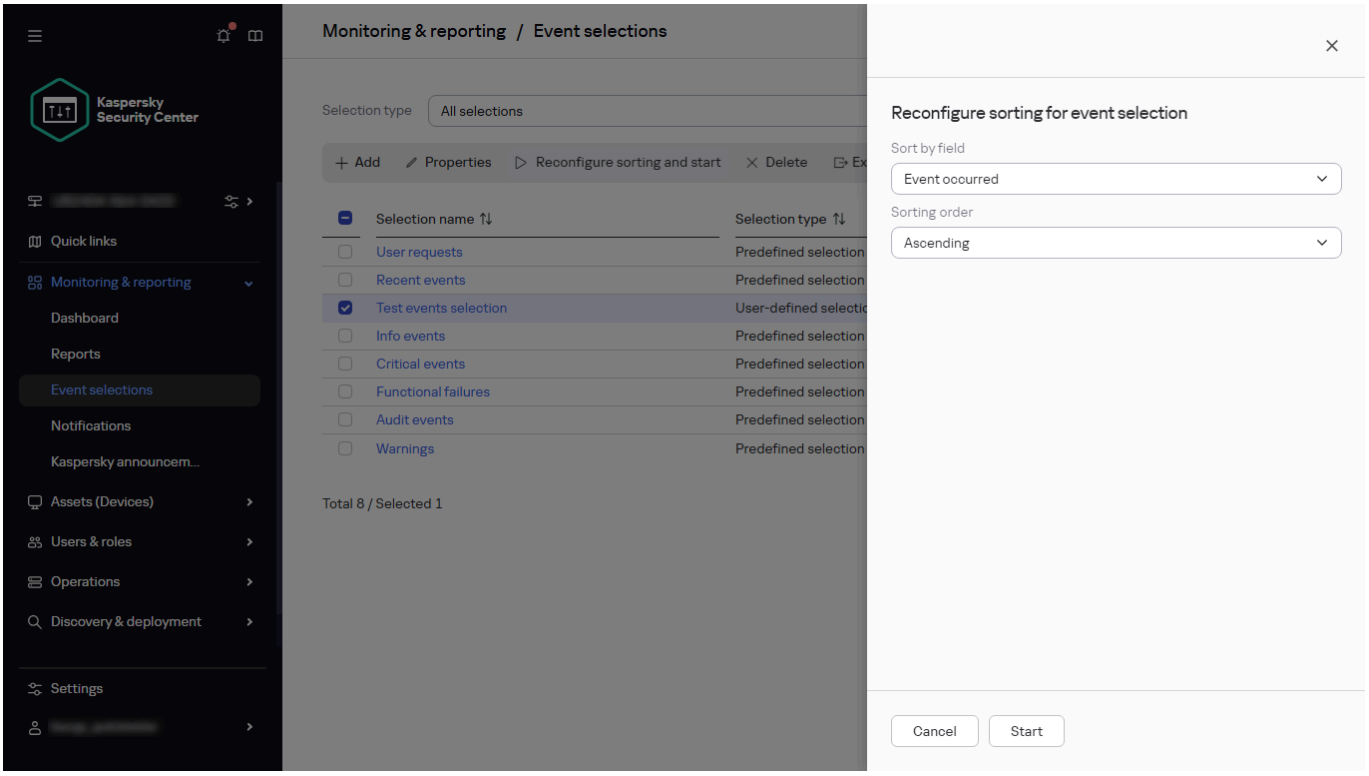
Список выборок событий

3. Выполните одно из следующих действий:

- Чтобы настроить сортировку для результатов выборки событий:

  a. Нажмите на кнопку **Изменить сортировку и запустить**.

  b. В отобразившемся окне **Изменить сортировку для выборки событий** укажите параметры сортировки.

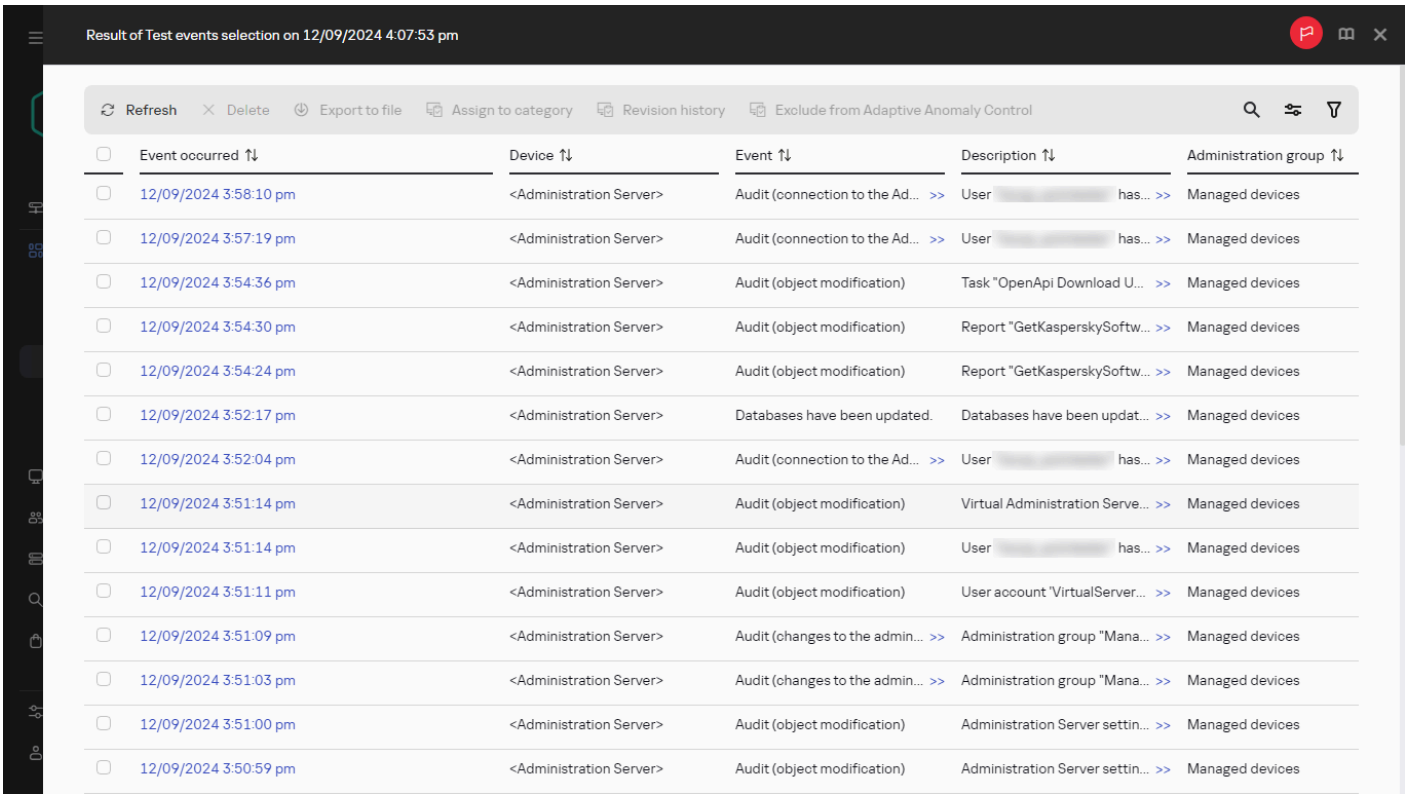


Указание параметров сортировки выборки событий

  a. Нажмите на имя выборки.

- В противном случае, если вы хотите просмотреть список событий так, как они хранятся на Сервере администрирования, нажмите на название выборки.

Отобразится результат выборки событий.



Результат выборки событий

Экспорт выборки событий

Open Single Management Platform позволяет сохранить выборку событий и ее параметры в файл KLO. Вы можете использовать файл KLO для импорта сохраненной выборки событий как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

Обратите внимание, что можно удалять только определенные пользователем выборки событий. Набор выборок событий, заданных по умолчанию в Open Single Management Platform (предопределенные выборки), не может быть сохранен в файл.

Чтобы экспортировать выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг → Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется экспортировать.

   Невозможно экспортировать несколько выборок событий одновременно. Если вы выберете более одной выборки, кнопка **Экспортировать** будет неактивна.
3. Нажмите на кнопку **Экспортировать**.
4. В открывшемся окне **Сохранить как** укажите имя и путь к файлу выборки событий, а затем нажмите на кнопку **Сохранить**.

   Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл выборки событий автоматически сохраняется в папку **Загрузки**.

Импорт выборки событий

Open Single Management Platform позволяет импортировать выборку событий из файла KLO. Файл KLO содержит экспортированную выборку событий и ее параметры.

Чтобы импортировать выборку событий:

1. В главном окне приложения перейдите в раздел **Мониторинг → Выборки событий**.
2. Нажмите на кнопку **Импортировать**, чтобы выбрать файл выборки событий, который вы хотите импортировать.
3. В открывшемся окне укажите путь к файлу KLO и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл выборки событий.

   Начнется обработка выборки событий.

Появится уведомление с результатами импорта. Если выборка событий импортирована, вы можете перейти по ссылке **Просмотреть сведения об импорте**, чтобы просмотреть свойства выборки.

После успешного импорта выборка событий отображается в списке выборок. Также импортируются параметры выборки событий.

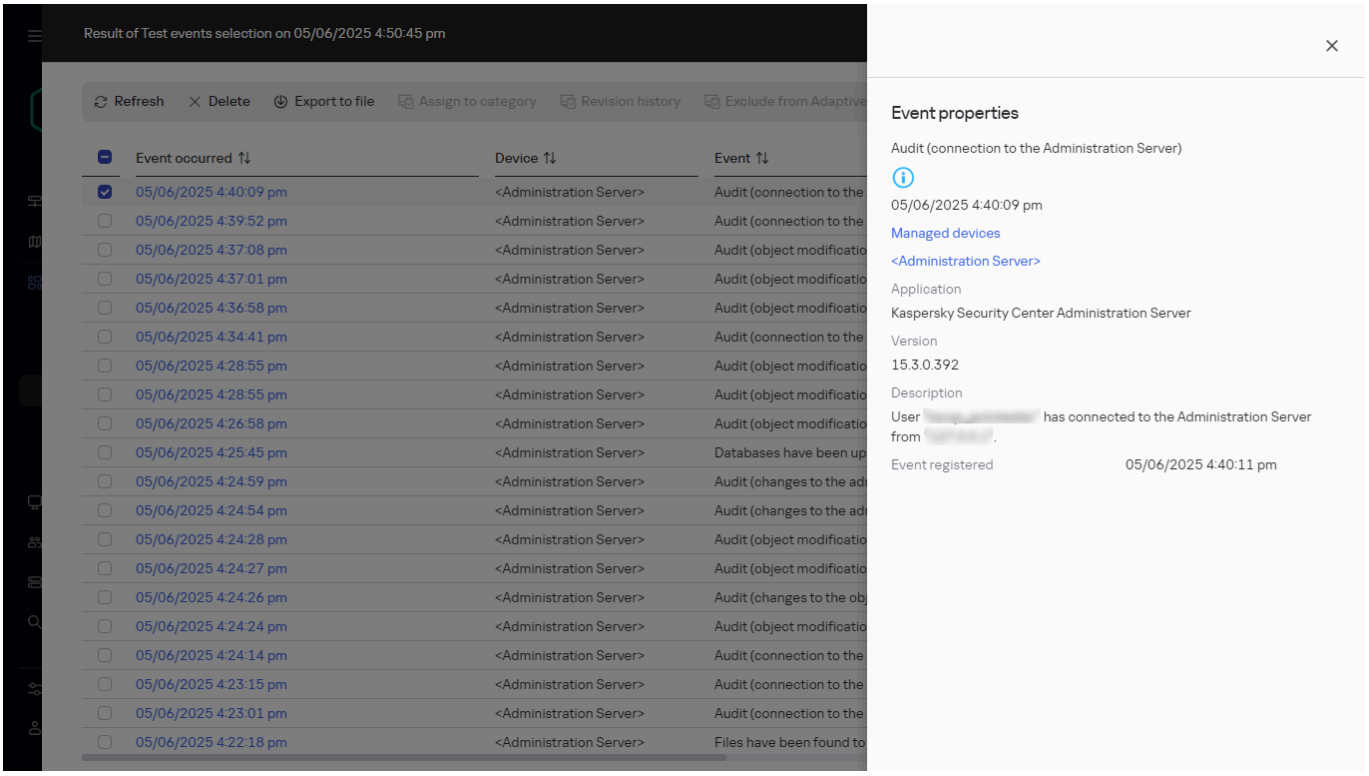
Если имя новой импортированной выборки событий идентично имени существующей выборки, имя импортированной выборки расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Просмотр информации о событии

Чтобы просмотреть детальную информацию о событии:

1. Запустите выборку событий.
2. Нажмите на требуемое событие.

Откроется окно **Свойства события**.



Окно свойств событий

3. В открывшемся окне можно выполнить следующие действия:

   - Просмотреть информацию выбранного события.
   - Перейти к устройству, на котором возникло событие.
   - Перейти к группе администрирования, содержащей устройство, на котором возникло событие.
   - Для события, связанного с задачей, перейдите в свойства задачи.

Экспорт событий в файл

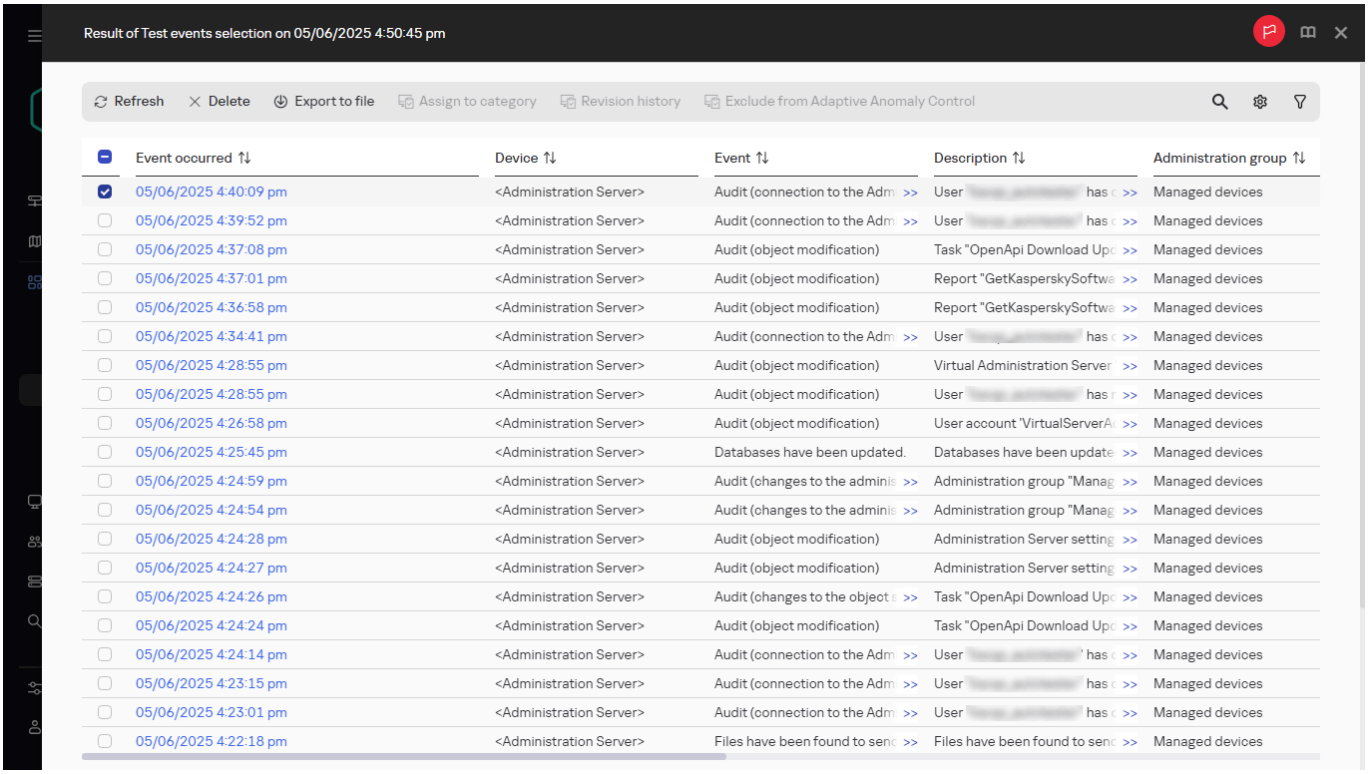
Open Single Management Platform позволяет сохранять события в файл формата CSV или TXT.

Чтобы экспортировать события из выборки событий:

1. В главном окне приложения перейдите в раздел **Мониторинг → Выборки событий**.
2. Нажмите на имя требуемой выборки.

3. Выберите события:

- Если вы хотите экспортировать одно или несколько событий, установите флажки рядом с ними.
- Если вы хотите экспортировать все события на текущей странице, установите флажок над списком событий и нажмите **Выбрать все на текущей странице**.
- Если вы хотите экспортировать все события из выборки, установите флажок над списком событий и нажмите **Выбрать все**.



Результат выборки событий

4. Нажмите на кнопку **Экспорт** и выберите **Экспортировать в CSV** или **Экспортировать в TXT**.

Чтобы экспортировать события из списка событий на устройстве:

1. Откройте список устройств.
   - Для управляемых устройств: **Управление активами** → **Управляемые устройства**.
   - Для нераспределенных устройств: **Управление активами** → **Нераспределенные устройства**.
2. В списке устройств нажмите на ссылку с названием нужного устройства и перейдите на вкладку **События**.

3. Выберите события:

   - Если вы хотите удалить одно или несколько событий, установите рядом с ними флажки.
   - Если вы хотите удалить все события на текущей странице, установите флажок над списком событий и выберите параметр **Выбрать все на текущей странице**.
   - Если вы хотите удалить все события из выборки, установите флажок над списком событий и выберите параметр **Выбрать все**.

4. Нажмите на кнопку **Экспорт** и выберите **Экспортировать в CSV** или **Экспортировать в TXT**.

   Вся информация о выбранных событиях, включенных в таблицу, будет экспортирована.

Просмотр истории объекта из события

Из события создания или события изменения объекта, которое поддерживает управление ревизиями, вы можете перейти к истории ревизий объекта.

Чтобы просмотреть историю объекта из события:

1. Запустите выборку событий.
2. Установите флажок рядом с требуемым событием.
3. Нажмите на кнопку **История ревизий**.

   Откроется история ревизий объекта.

Хранение информации о событиях для задач и политик

В этом разделе приведены расчеты, связанные с хранением событий в базе данных Сервера администрирования, и даны рекомендации, как минимизировать количество событий и таким образом снизить нагрузку на Сервер администрирования.

По умолчанию в свойствах каждой задачи и каждой политики указано сохранение в журнале всех событий, связанных с выполнением задачи и применением политики.

Однако если задача запускается достаточно часто (например, более одного раза в неделю) и на достаточно большом количестве устройств (например, более 10 000), количество событий может оказаться слишком большим, и события могут заполнить базу данных. В таком случае рекомендуется указать в свойствах задачи один из двух других вариантов:

- **Сохранять события, связанные с ходом выполнения задачи**. В этом случае с каждого устройства, на котором выполнена задача, в базу данных поступает только информация о запуске задачи, о ее ходе и о ее выполнении (успешном, с предупреждением либо с ошибкой).
- **Сохранять только результат выполнения задачи**. В этом случае с каждого устройства, на котором выполнена задача, в базу данных поступает только информация о выполнении задачи (успешном, с предупреждением либо с ошибкой).

Если политика определена для достаточно большого количества устройств (например, более 10 000), количество событий также может оказаться слишком большим, и события могут заполнить базу данных. В таком случае рекомендуется выбрать в свойствах политики только наиболее важные события и включить их сохранение. Сохранение всех других событий рекомендуется отключить.

Таким образом вы уменьшаете количество событий в базе данных, увеличиваете скорость работы сценариев, связанных с анализом таблицы событий в базе данных, и снижаете риск вытеснения критических событий большим количеством событий.

Вы также можете уменьшить срок хранения событий, связанных с задачей или политикой. По умолчанию этот срок составляет семь дней для событий, связанных с задачей, и 30 дней для событий, связанных с политикой. При изменении срока хранения событий принимайте в расчет порядок работы, принятый в вашей организации, и количество времени, которое системный администратор может уделять анализу каждого события.

Вносить изменения в параметры хранения событий целесообразно в любом из следующих случаев:

- события об изменении промежуточных состояний групповых задач и о применении политик занимают значительный процент всех событий в базе данных Kaspersky SIEM Cloud;
- в журнале событий операционной системы появляются записи об автоматическом удалении событий при превышения заданного лимита на общее число событий, хранимых в базе данных.

Выберите параметры регистрации событий, исходя из того, что оптимальное количество событий, поступающих с одного устройства в день, не должно превышать 20. Вы можете немного увеличить максимальное количество событий, если это необходимо, но только в том случае, если количество устройств в вашей сети относительно невелико (менее 10 000).

Удаление событий

Чтобы удалить события из выборки событий:

1. Запустите выборку событий.
2. Выберите события:
   - Если вы хотите удалить одно или несколько событий, установите рядом с ними флажки.
   - Если вы хотите удалить все события на текущей странице, установите флажок над списком событий и выберите параметр **Выбрать все на текущей странице**.
   - Если вы хотите удалить все события из выборки, установите флажок над списком событий и выберите параметр **Выбрать все**.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **Удалить**.

Чтобы удалить события из списка событий устройства:

1. Откройте список устройств.
   - Для управляемых устройств: **Управление активами** → **Управляемые устройства**.
   - Для нераспределенных устройств: **Управление активами** → **Нераспределенные устройства**.

2. В списке устройств нажмите на ссылку с названием нужного устройства и перейдите на вкладку **События**.

3. Выберите события:

   - Если вы хотите удалить одно или несколько событий, установите рядом с ними флажки.
   - Если вы хотите удалить все события на текущей странице, установите флажок над списком событий и выберите параметр **Выбрать все на текущей странице**.
   - Если вы хотите удалить все события из выборки, установите флажок над списком событий и выберите параметр **Выбрать все**.

4. Нажмите **Удалить** и подтвердите действие.

5. В появившемся окне нажмите на кнопку **Удалить**.

   Выбранные события удалены и не могут быть восстановлены.

Удаление выборок событий

Можно удалять только пользовательские выборки событий. Предопределенные выборки событий невозможно удалить.

Чтобы удалить выборки событий:

1. В главном окне приложения перейдите в раздел **Мониторинг → Выборки событий**.

2. Установите флажки напротив выборок событий, которые требуется удалить.

3. Нажмите на кнопку **Удалить**.

4. В появившемся окне нажмите на кнопку **OK**.

   Выборка событий будет удалена.

Настройка срока хранения события

Kaspersky SIEM Cloud позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования. Возможно, вам нужно хранить некоторые события в течение более длительного или более короткого периода, чем указано по умолчанию. Вы можете изменить срок хранения события по умолчанию.

Если вас не интересует сохранение каких-либо событий в базе данных Сервера администрирования, вы можете выключить соответствующий параметр в политике Сервера администрирования, политике приложения "Лаборатории Касперского" или в свойствах Сервера администрирования (только для событий Сервера администрирования). Это уменьшит количество типов событий в базе данных.

Чем больше срок хранения события, тем быстрее база данных достигает максимального размера. Однако более длительный срок хранения события позволяет выполнять задачи мониторинга и просматривать отчеты в течение более длительного периода.

Чтобы задать срок хранения события в базе данных Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на название требуемой политики.

   Вы можете выбрать политику управляемого приложения "Лаборатории Касперского", Агента администрирования или Сервера администрирования. Для Сервера администрирования вы можете настроить срок хранения событий, нажав на имя Сервера администрирования.
3. Выберите вкладку **Настройка событий**.

   Отображается раздел **Критическое** со списком связанных событий. При необходимости вы можете перейти в раздел **Отказ функционирования**, **Предупреждение** или **Информационное сообщение**.
4. В списке типов событий на правой панели перейдите по ссылке с названием события, срок хранения которого вы хотите изменить.

   В открывшемся окне в разделе **Регистрация событий** включите переключатель **Хранить в базе данных Сервера администрирования в течение (сут)**.
5. В поле редактирования под переключателем укажите количество дней для сохранения события.
6. Если вы не хотите сохранять событие в базе данных Сервера администрирования, выключите параметр **Хранить в базе данных Сервера администрирования в течение (сут)**.

   > Если вы настраиваете события Сервера администрирования в окне свойств Сервера администрирования и если параметры событий заблокированы в политике Сервера администрирования, вы не сможете изменить значение срока хранения события.
7. Нажмите на кнопку **ОК**, а затем после того, как правая панель закроется, нажмите на кнопку **Сохранить**.

   Окно свойств политики закроется.

Теперь, когда Сервер администрирования получает и сохраняет события выбранного типа, они будут иметь измененный срок хранения. Сервер администрирования не изменяет срок хранения ранее полученных событий.

Блокировка частых событий

В этом разделе представлена информация об управлении блокировкой частых событий и об отмене блокировки частых событий.

О блокировке частых событий

Управляемое приложение, например Kaspersky Endpoint Security для Linux, установленное на одном или нескольких управляемых устройствах, может отправлять на Сервер администрирования множество однотипных событий. Прием частых событий может привести к перегрузке базы данных Сервера администрирования и перезаписи других событий. Сервер администрирования начинает блокировать наиболее частые события, когда количество всех полученных событий превышает установленное ограничение для базы данных.

Сервер администрирования автоматически блокирует получение частых событий. Вы не можете заблокировать частые события самостоятельно или выбрать, какие события заблокировать.

Чтобы узнать, заблокировано ли событие, вы можете просмотреть список уведомлений или просмотреть, присутствует ли это событие в свойствах Сервера администрирования в разделе **Блокировка частых событий**. Если событие заблокировано, можно выполнить следующие действия:

- Если вы хотите предотвратить перезапись базы данных, вы можете продолжать блокировать получение событий такого типа.
- Если вы хотите, например, выяснить причину отправки частых событий на Сервер администрирования, вы можете разблокировать частые события и в любом случае продолжить получение событий этого типа.
- Если вы хотите продолжать получать частые события до тех пор, пока они снова не будут заблокированы, вы можете отменить блокировку частых событий.

Управление блокировкой частых событий

Сервер администрирования автоматически блокирует получение частых событий, но вы можете разблокировать и продолжать получать частые события. Также можно заблокировать получение частых событий, которые вы разблокировали ранее.

Чтобы управлять блокировкой частых событий:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Блокировка частых событий**.

3. В разделе **Блокировка частых событий**:

   - Если вы хотите разблокировать прием частых событий:

     a. Выберите частые события, который нужно разблокировать, и нажмите на кнопку **Исключить**.

     b. Нажмите на кнопку **Сохранить**.

   - Если вы хотите заблокировать прием частых событий:

     a. Выберите частые события, которые вы хотите заблокировать и нажмите на кнопку **Заблокировать**.

     b. Нажмите на кнопку **Сохранить**.

Сервер администрирования принимает разблокированные частые события и не принимает заблокированные частые события.

Отмена блокировки частых событий

Вы можете отменить блокировку частых событий и начать получение событий до тех пор, пока Сервер администрирования снова не заблокирует эти частые события.

Чтобы отменить блокировку частых событий:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Блокировка частых событий**.

3. В разделе **Блокировка частых событий** нажмите строку частого события, для которого вы хотите отменить блокировку.

4. Нажмите на кнопку **Отменить блокировку**.

Частое событие удаляется из списка частых событий. Сервер администрирования будет получать события этого типа.

Обработка и хранение событий на Сервере администрирования

Информация о событиях, возникших в работе приложения и управляемых устройств, сохраняется в базе данных Сервера администрирования. Каждое событие относится к определенному типу и уровню важности (*Критическое событие*, *Отказ функционирования*, *Предупреждение*, *Информационное сообщение*). В зависимости от условий, при которых произошло событие, приложение может присваивать событиям одного типа разные уровни важности.

Вы можете просматривать типы и уровни важности событий в разделе **Настройка событий** окна свойств Сервера администрирования. В разделе **Настройка событий** вы также можете настроить параметры обработки каждого события Сервером администрирования:

- регистрацию событий на Сервере администрирования и в журналах событий операционной системы на устройстве и на Сервере администрирования;

- способ уведомления администратора о событии (например, SMS, сообщение электронной почты).

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, приложение вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Приложение проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 000 больше указанного максимального значения, приложение удаляет самые старые события, чтобы осталось только указанное максимальное количество событий.

Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий операционной системы. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления. По умолчанию очередь событий ограничена 20 000 событиями. Вы можете настроить ограничение очереди, изменив значение флага KLEVP_MAX_POSTPONED_CNT.

Уведомления и статусы устройств

В этом разделе содержится информация о том, как просматривать уведомления, настраивать доставку уведомлений, использовать статусы устройств и включать изменение статусов устройств.

Об уведомлениях

Уведомления информируют вас о важных событиях и помогают быстро отреагировать на них, выполнив рекомендуемые действия или другие соответствующие действия.

В зависимости от выбранного способа уведомления доступны следующие типы уведомлений:

- экранные уведомления;
- уведомление по SMS;
- уведомление по электронной почте;
- уведомление запуском исполняемого файла или скрипта.

Экранные уведомления

Экранные уведомления доступны в раскрывающейся панели, которая открывается при нажатии на значок уведомлений ( ), и в Центре уведомлений. Им присваивается один из следующих уровней важности: **Критическая**, **Предупреждение**, **Информационное сообщение** и **Успешно**.

Красная точка на значке означает, что есть непрочитанные уведомления.

Экранные уведомления сгруппированы по следующим типам:

- **Требуется внимание**

  Уведомления, требующие вашего внимания. Уведомления с уровнем важности **Критический** отображаются на главной информационной панели в дополнение к Центру уведомлений.

- **Система**

  Системные уведомления. Они разделены на следующие категории:

  - **Развертывание**
  - **Устройства**

- **Защита**
- **Обновления** (включая уведомления о доступных для скачивания приложений "Лаборатории Касперского", уведомления о скачанных обновлениях антивирусных баз и уведомления об устройствах, требующих перезагрузки после обновления Агента администрирования)
- **Защита от эксплойтов**
- **Сервер администрирования** (включает только события, связанные с Сервером администрирования)

- **Объявления**

  Уведомления, содержащие информацию о вашей версии Kaspersky SIEM Cloud и управляемых приложениях, установленных на управляемых устройствах.

Вы можете контролировать сеть вашей организации, просматривая уведомления на экране и отвечая на них в режиме реального времени.

Уведомления по электронной почте, SMS и запуском исполняемого файла или скрипта

Kaspersky SIEM Cloud позволяет вам контролировать сеть вашей организации, отправляя уведомления о событиях, которые вы считаете важными. Для любого события вы можете настроить уведомления по электронной почте, SMS или запустив исполняемый файл или скрипт.

Получив уведомление по SMS или по электронной почте, вы можете принять решение о своем ответе на событие. Этот ответ должен быть наиболее подходящим для сети вашей организации. Запустив исполняемый файл или скрипт, вы заранее определяете ответ на событие. Вы также можете рассмотреть запуск исполняемого файла или скрипта в качестве основного ответа на событие. После запуска исполняемого файла вы можете предпринять другие шаги для ответа на событие.

Просмотр уведомлений, требующих внимания

Уведомления, требующие внимания, информируют вас о событиях, которые могут потребовать вашего участия. Им присваивается один из следующих уровней важности: **Критическая**, **Предупреждение**, **Информационное сообщение** и **Успешно**.

Уведомления с уровнем важности **Критическая** отображаются в Web Console в дополнении к уведомлениям из Центра уведомлений. Если есть несколько критичных уведомлений, Web Console отображает одно уведомление, показывающее общее количество предельных уведомлений.

Вы можете просмотреть уведомления, требующие внимания, одним из следующих способов:

- В раскрывающейся панели.

  В раскрывающейся панели отображаются только непрочитанные уведомления, требующие внимания. Если нет непрочитанных уведомлений, требующих внимания, вкладка **Требуется внимание** не отображается.

- В Центре уведомлений.

  Центр уведомлений отображает все уведомления, требующие внимания, включая прочитанные и непрочитанные уведомления. Если нет уведомлений, требующих внимания, вкладка **Требуется внимание** не отображается.

Чтобы просмотреть уведомления, требующие внимания, в раскрывающейся панели:

1. В верхней части окна приложения Web Console нажмите на значок уведомления ( ).

   Откроется панель **Уведомления**.

2. На вкладке **Требуется внимание** просмотрите непрочитанные уведомления.

3. При необходимости отметьте требуемые уведомления как прочитанные одним из следующих способов:

   - Чтобы отметить уведомление как прочитанное, нажмите на значок закрытия (×) рядом с уведомлением.

   - Чтобы отметить все объявления как прочитанные, нажмите на кнопку **Отметить как прочитанное**.

После просмотра и отметки уведомлений, требующих внимания, вкладка **Требуется внимание** больше не отображается в раскрывающейся панели **Уведомления**. Вы можете просмотреть все уведомления, требующие внимания, в Центре уведомлений.

Чтобы просмотреть уведомления, требующие внимания, в Центре уведомлений:

1. В верхней части окна приложения Web Console нажмите на значок уведомления ( ).

2. В открывшейся панели **Уведомления** нажмите на кнопку **Перейти в Центр уведомлений**.

   Откроется окно **Центр уведомлений**.

3. На вкладке **Требуется внимание** выберите один из следующих разделов:

   - **Все уведомления, требующие внимания** – отображаются все уведомления, требующие внимания, независимо от их уровня важности.

   - **Критическая** – отображаются уведомления с уровнем важности **Критическая**.

   - **Предупреждение** – отображаются уведомления с уровнем важности **Предупреждение**.

   - **Информационное сообщение** – отображаются уведомления с уровнем важности **Информационное сообщение**.

4. Чтобы отображать только непрочитанные уведомления, включите переключатель **Показать только непрочитанное**.

5. В списке уведомлений нажмите на уведомление, чтобы просмотреть его текст. Полный текст уведомления отображается в панели сведений справа.

   Когда вы просматриваете уведомление, оно автоматически отмечается как прочитанное.

6. Чтобы отметить уведомления как прочитанные вручную, выполните одно из следующих действий:

   - Чтобы отметить уведомление как прочитанное, выберите его в списке уведомлений и нажмите на кнопку **Отметить как прочитанное**.
   - Чтобы отметить все уведомления как прочитанные, нажмите на кнопку **Отметить как прочитанное**.

7. При необходимости вы можете отметить уведомление как непрочитанное, выбрав его в списке уведомлений и нажав на кнопку **Отметить как непрочитанное**.

Уведомления, требующие внимания, просмотрены.

Просмотр системных уведомлений

Системные уведомления информируют вас о событиях, связанных с Web Console и с управляемыми устройствами. Системные уведомления сгруппированы по типам и имеют один из следующих уровней важности: **Критическая**, **Предупреждение**, **Информационное сообщение** и **Успешно**.

Вы можете просмотреть системные уведомления одним из следующих способов:

- В раскрывающейся панели.
- В Центре уведомлений.

Чтобы просмотреть системные уведомления, в раскрывающейся панели:

1. В верхней части окна приложения Web Console нажмите на значок уведомления ( ).

   Откроется панель **Уведомления**.

2. На вкладке **Система** просмотрите непрочитанные уведомления.

3. При необходимости отметьте системные уведомления как прочитанные одним из следующих способов:

   - Чтобы отметить уведомление как прочитанное, нажмите на значок закрытия (×) рядом с уведомлением.
   - Чтобы отметить все объявления как прочитанные, нажмите на кнопку **Отметить как прочитанное**.

После того как вы просмотрите все системные уведомления и отметите их как прочитанные, в раскрывающейся панели **Уведомления** отобразится сообщение об отсутствии новых уведомлений. Вы можете просмотреть все системные уведомления, прочитанные и непрочитанные, в Центре уведомлений.

Чтобы просмотреть системные уведомления в Центре уведомлений:

1. В верхней части окна приложения Web Console нажмите на значок уведомления ( ).

2. В открывшейся панели **Уведомления** нажмите на кнопку **Перейти в Центр уведомлений**.

   Откроется окно **Центр уведомлений**.

3. На вкладке **Система** выберите один из следующих разделов:

   - **Все системные уведомления**
   - **Развертывание**
   - **Устройства**
   - **Защита**
   - **Обновления**
   - **Защита от эксплойтов**
   - **Сервер администрирования**

4. Чтобы отображать только непрочитанные уведомления, включите переключатель **Показать только непрочитанное**.

5. В списке уведомлений нажмите на уведомление, чтобы просмотреть его текст. Полный текст уведомления отображается в панели сведений справа.

   Когда вы просматриваете уведомление, оно автоматически отмечается как прочитанное.

6. Чтобы отметить уведомления как прочитанные вручную, выполните одно из следующих действий:

   - Чтобы отметить уведомление как прочитанное, выберите его в списке уведомлений и нажмите на кнопку **Отметить как прочитанное**.
   - Чтобы отметить все уведомления как прочитанные, нажмите на кнопку **Отметить как прочитанное**.

7. При необходимости вы можете отметить уведомление как непрочитанное, выбрав его в списке уведомлений и нажав на кнопку **Отметить как непрочитанное**.

Системные уведомления просмотрены.

Просмотр объявлений

Объявления – это тип уведомлений, которые содержат информацию о вашей версии Kaspersky SIEM Cloud и версиях приложений "Лаборатории Касперского", установленных на ваших управляемых устройствах. Отображаются только объявления, относящиеся к текущему подключенному Серверу администрирования и приложениям "Лаборатории Касперского", установленным на управляемых устройствах этого Сервера администрирования. Объявления отображаются отдельно для каждого Сервера администрирования, главного, подчиненного или виртуального.

Если несколько администраторов используют Kaspersky SIEM Cloud и устанавливают разные языки интерфейса, Kaspersky SIEM Cloud отображает объявления "Лаборатории Касперского" на всех языках, используемых администраторами. При изменении языка интерфейса объявления "Лаборатории Касперского" на выбранном языке автоматически добавляются в раздел после выхода из Web Console и повторного входа.

Для получения объявлений "Лаборатории Касперского" Сервер администрирования должен иметь подключение к интернету.

Объявления включают следующие типы информации:

- Информация, связанная с безопасностью.

  Объявления, связанные с безопасностью, включают критические обновления, исправления для уязвимостей и рекомендации по устранению проблем в приложениях "Лаборатории Касперского". Объявления, связанные с безопасностью, включены по умолчанию. Если вы не хотите получать объявления, связанные с безопасностью, вы можете выключить эту функцию.

  Вы не можете отключить объявления, связанные с безопасностью, в пробном режиме Kaspersky SIEM Cloud.

  Для предоставления информации, которая соответствует вашей конфигурации защиты сети, Kaspersky SIEM Cloud отправляет данные на облачные серверы "Лаборатории Касперского" и получает только те объявления, которые относятся к приложениям "Лаборатории Касперского", установленным в вашей сети. Данные, которые могут быть отправлены на серверы, описаны в Лицензионном соглашении, которое вы принимаете при создании рабочей области Open Single Management Platform.

- Маркетинговая информация.

  Маркетинговая объявления включают специальные предложения, новости о приложениях и рекламу приложений "Лаборатории Касперского". Маркетинговые объявления доступны, только если включен Kaspersky Security Network (KSN). Вы можете выключить маркетинговые объявления, выключив KSN.

  Чтобы предоставить информацию, которая может помочь вам защитить ваши сетевые устройства и выполнять повседневные задачи, Kaspersky SIEM Cloud отправляет данные на облачные серверы "Лаборатории Касперского" и получает соответствующие объявления. Данные, которые могут быть отправлены на серверы, описан в разделе "Обрабатываемые данные" Положения о KSN.

Объявлениям присваивается один из следующих уровней важности: **Критическая**, **Предупреждение**, **Информационное сообщение** и **Успешно**.

Вы можете просмотреть объявления одним из следующих способов:

- В раскрывающейся панели.
- В Центре уведомлений.

Чтобы просмотреть объявления в раскрывающейся панели:

1. В верхней части окна приложения Web Console нажмите на значок уведомления ( ).

   Откроется панель **Уведомления**.

2. На вкладке **Объявления** просмотрите непрочитанные уведомления.

3. При необходимости отметьте объявления как прочитанные одним из следующих способов:

   - Чтобы отметить уведомление как прочитанное, нажмите на значок закрытия (×) рядом с уведомлением.
   - Чтобы отметить все объявления как прочитанные, нажмите на кнопку **Отметить как прочитанное**.

   После того как вы просмотрите все уведомления и отметите их как прочитанные, в раскрывающейся панели **Уведомления** отобразится сообщение об отсутствии новых уведомлений. Вы можете просмотреть все объявления, прочитанные и непрочитанные, в Центре уведомлений.

Чтобы просмотреть объявления в Центре уведомлений:

1. В верхней части окна приложения Web Console нажмите на значок уведомления ( ).

2. В открывшейся панели **Уведомления** нажмите на кнопку **Перейти в Центр уведомлений**.

   Откроется окно **Центр уведомлений**.

3. На вкладке **Объявления** выберите один из следующих разделов:

   - **Все объявления** – отображаются все уведомления, независимо от их уровня важности.
   - **Критическая** – отображаются уведомления с уровнем важности **Критическая**.
   - **Предупреждение** – отображаются уведомления с уровнем важности **Предупреждение**.
   - **Информационное сообщение** – отображаются уведомления с уровнем важности **Информационное сообщение**.

4. Чтобы отображать только непрочитанные уведомления, включите переключатель **Показать только непрочитанное**.

5. В списке уведомлений нажмите на уведомление, чтобы просмотреть его текст. Полный текст уведомления отображается в панели сведений справа.

   Когда вы просматриваете уведомление, оно автоматически отмечается как прочитанное.

6. Чтобы отметить уведомления как прочитанные вручную, выполните одно из следующих действий:

   - Чтобы отметить уведомление как прочитанное, выберите его в списке уведомлений и нажмите на кнопку **Отметить как прочитанное**.

   - Чтобы отметить все уведомления как прочитанные, нажмите на кнопку **Отметить как прочитанное**.

7. При необходимости вы можете отметить уведомление как непрочитанное, выбрав его в списке уведомлений и нажав на кнопку **Отметить как непрочитанное**.

Объявления просмотрены.

Просмотр экранных уведомлений

Вы можете просматривать экранные уведомления тремя способами:

- В разделе **Мониторинг → Уведомления**. Здесь вы можете просмотреть уведомления, относящиеся к предопределенным категориям.

- В отдельном окне, которое можно открыть независимо от того, какой раздел вы используете в данный момент. В этом случае вы можете отметить уведомления как просмотренные.

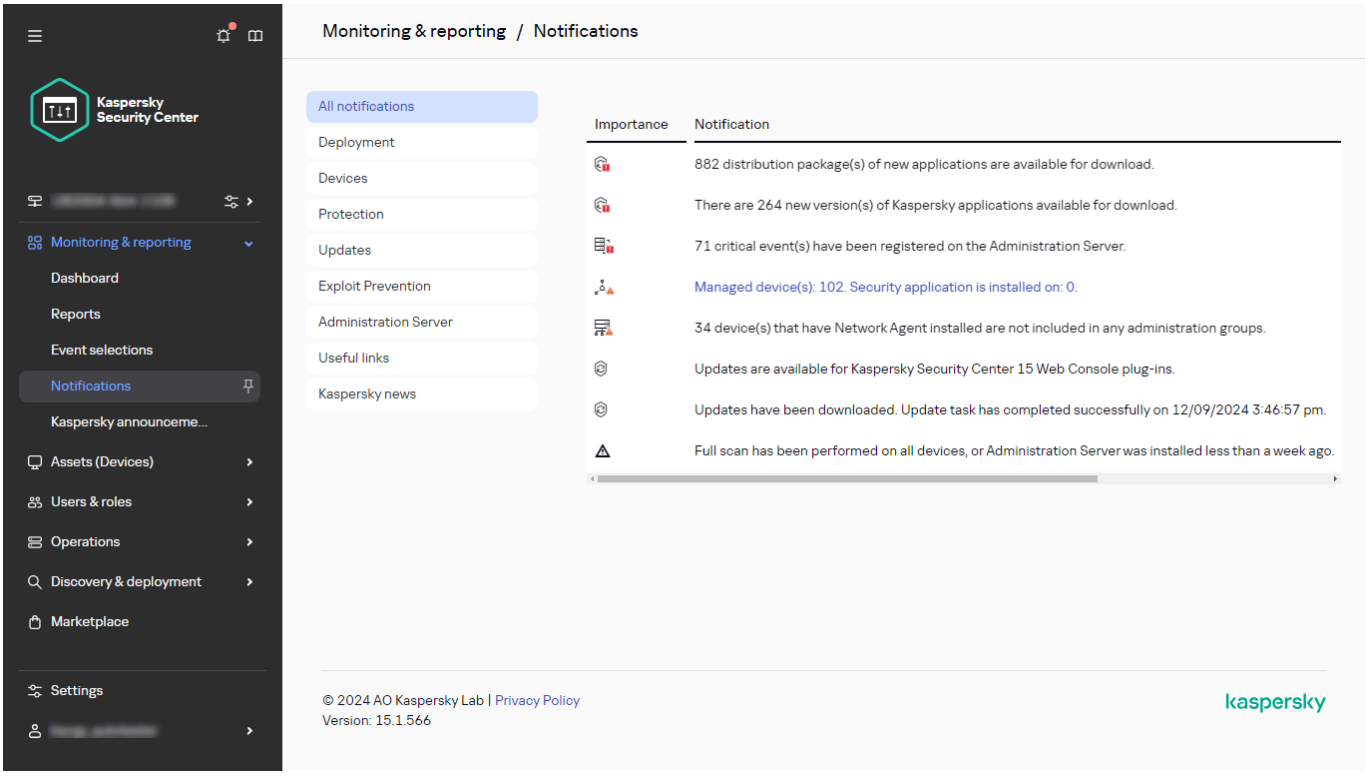
- В виджете **Уведомления, выбранные по уровню важности** в разделе **Мониторинг → Панель мониторинга**. В этом виджете вы можете просматривать только уведомления с уровнями важности *Критическое* и *Предупреждение*.

Вы можете выполнять действия, например, вы можете ответить на событие.

Чтобы просмотреть уведомления предопределенной категории:

1. В главном окне приложения перейдите в раздел **Мониторинг → Уведомления**.

   На левой панели выбрана категория **Все уведомления**, а справа отображаются все уведомления.



Список уведомлений

2. На левой панели выберите одну из следующих категорий:

   - **Развертывание**.
   - **Устройства**.
   - **Защита**.
   - **Обновления**.

     Это уведомление включает в себя уведомления о доступных для скачивания приложениях "Лаборатории Касперского", уведомления об обновлении антивирусных баз, которые были загружены, а также уведомления об устройствах, если есть, которые требуют перезагрузки после обновления Агента администрирования.

   - **Защита от эксплойтов**.
   - **Сервер администрирования**.

     Это уведомление включает в себя события, относящиеся только к Серверу администрирования.

   - **Полезные ссылки**.

     Это уведомление включает в себя ссылки на ресурсы "Лаборатории Касперского", например, ссылка на Службу технической поддержки "Лаборатории Касперского", на форум "Лаборатории Касперского", на страницу продления лицензии или на Вирусную энциклопедию.

В списке уведомлений отобразится выбранная категория. Список содержит следующее:

- Значок, относящийся к теме уведомления: развертывание (), защита (), обновления (), управление устройствами (), Защита от эксплойтов (), Сервер администрирования ().
- Уровень важности уведомления. Отображаются уведомления со следующими уровнями важности: **Критические уведомления** (), **Предупреждающие уведомления** (), **Информационные уведомления**. Уведомления в списке сгруппированы по уровню важности.
- **Уведомление**. Здесь содержится описание уведомления.
- **Действие**. Здесь содержится ссылка на быстрое действие, которое рекомендуется выполнить. Например, по этой ссылке вы можете перейти к хранилищу и установить приложение безопасности на устройства, просмотреть список устройств или список событий. После того как вы выполнили рекомендуемое действие для уведомления, этому уведомлению присваивается статус *Просмотрено*.
- **Зарегистрированный статус**. Здесь содержится количество дней или часов, прошедших с даты регистрации уведомления на Сервере администрирования.

Чтобы просмотреть экранные уведомления в отдельном окне по уровню важности:

1. Нажмите на значок флага () в правом верхнем углу OSMP Console.

   Если около значка флажка есть красная точка, значит, есть непросмотренные уведомления.

   Откроется окно со списком уведомлений. По умолчанию выбрана вкладка **Все уведомления** и отображаются уведомления, сгруппированные по уровням важности: *Критические уведомления*, *Предупреждающие уведомления* и *Информационные уведомления*.

2. Выберите вкладку **Система**.

   Отображается список уведомлений с уровнями важности *Критические уведомления* ( ) и *Предупреждающие уведомления* (). Список уведомление включает следующее:

   - Цветной индикатор. Критические уведомления отмечены красным. Предупреждающие уведомления отмечены желтым.
   - Значок, относящийся к теме уведомления: развертывание (), защита (), обновления (), управление устройствами (), Защита от эксплойтов (), Сервер администрирования ().
   - Описание уведомления.
   - Значок флажка. Серый флаг используется для уведомлений, которым присвоен статус *Не просмотрено*. Когда вы выбираете серый флаг и назначаете статус *Просмотрено* для уведомления, цвет флажка изменится на белый.
   - Ссылка на рекомендуемое действие. Когда вы выполняете рекомендуемое действие, переходя по ссылке, уведомлению присваивается статус *Просмотрено*.
   - Количество дней, прошедших с даты регистрации уведомления на Сервере администрирования.

3. Выберите вкладку **Больше**.

   Отображается список уведомлений с уровнем важности *Информационное уведомление*.

   Структура списка такая же, как и для списка на вкладке **Система** (описание приведено выше). Отличается только отсутствием цветного индикатора.

Вы можете фильтровать уведомления по датам, когда они были зарегистрированы на Сервере администрирования. Используйте флажок **Показать фильтр**, чтобы настроить фильтр.

Чтобы просмотреть экранные уведомления на виджете:

1. В разделе **Панель мониторинга** выберите **Добавить или восстановить виджет**.
2. В открывшемся окне нажмите на категорию **Другие**, выберите виджет **Уведомления, выбранные по уровню важности** и нажмите на кнопку Добавить.

   Виджет отображается на вкладке **Панель мониторинга**. По умолчанию на виджете отображаются уведомления с уровнем важности *Критическое*.

   Вы можете нажать на кнопку **Параметры** на виджете и изменить параметры виджета, чтобы просмотреть уведомления с уровнем важности *Предупреждающие уведомления*. Или вы можете добавить другой виджет: **Уведомления, выбранные по уровню важности** с уровнем важности *Предупреждающие уведомления*.

   Список уведомлений на виджете ограничен размером и включает только два уведомления. Эти два уведомления относятся к последним событиям.

Список уведомлений виджета включает следующее:

- Значок, относящийся к теме уведомления: развертывание (), защита (), обновления (), управление устройствами (), Защита от эксплойтов (), Сервер администрирования ().
- Описание уведомления со ссылкой на рекомендуемое действие. Когда вы выполняете рекомендуемое действие, переходя по ссылке, уведомлению присваивается статус *Просмотрено*.

- Количество дней или часов, прошедших с даты регистрации уведомления на Сервере администрирования.

- Ссылка на другие уведомления. Перейдите по ссылке к просмотру уведомлений в разделе **Уведомления** в разделе **Мониторинг**.

О статусах устройства

Kaspersky SIEM Cloud присваивает статус каждому управляемому устройству. Конкретный статус зависит от того, выполнены ли условия, определенные пользователем. В некоторых случаях при присваивании статуса устройству Kaspersky SIEM Cloud учитывает видимость устройства в сети (см. таблицу ниже). Если Kaspersky SIEM Cloud не находит устройство в сети в течение двух часов, видимость устройства принимает значение *Не в сети*.

Существуют следующие статусы:

- *Критический* или *Критический/Видим в сети*.

- *Предупреждение* или *Предупреждение/Видим в сети*.

- *OK* или *OK/Видим в сети*.

В таблице ниже приведены условия по умолчанию для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения.

Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Приложение безопасности не установлено	Агент администрирования установлен на устройстве, но не установлено приложение безопасности.	• Переключатель включен. • Переключатель выключен.
Обнаружено много вирусов	В результате работы задач поиска вирусов, например, задачи Поиск вирусов, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение.	Более 0.
Уровень постоянной защиты отличается от уровня, установленного администратором	Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства.	• Остановлена. • Приостановлена. • Выполняется.
Давно не выполнялся поиск вредоносного ПО	Устройство видимо в сети и на устройстве установлено приложение безопасности, но ни задача *Поиск вредоносного ПО*, ни задача локальной проверки не выполнялись больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня.
Базы устарели	Устройство видимо в сети и на устройстве установлено приложение безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня.
Давно не подключались	Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.	Более 1 дня.
Обнаружены активные угрозы	Количество необработанных объектов в папке **Активные угрозы** превышает указанное значение.	Более чем 0 штук.

Условие	Описание условия	Доступные значения
Требуется перезагрузка	Устройство видимо в сети, но приложение требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин.	Более чем 0 минут.
Установлены несовместимые приложения	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые приложения.	• Переключатель выключен. • Переключатель включен.
Обнаружены уязвимости в приложениях	Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи *Поиск уязвимостей и требуемых обновлений* на устройстве обнаружены уязвимости в приложениях с заданным уровнем критичности.	• Предельный. • Высокий. • Средний. • Игнорировать, если невозможно закрыть уязвимость. • Игнорировать, если обновление назначено к установке.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	• Переключатель выключен. • Переключатель включен.
Срок действия лицензии скоро истекает	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Менее чем 0 дней.
Давно не выполнялась проверка обновлений Центра обновления Windows	Устройство видимо в сети, но задача *Поиск уязвимостей и требуемых обновлений* не выполнялась больше указанного времени.	Более 1 дня.
Недопустимый статус шифрования	Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению.	• Не соответствует политике из-за отказа пользователя (только для внешних устройств). • Не соответствует политике из-за ошибки. • В процессе применения политики – требуется перезагрузка. • Не задана политика шифрования. • Не поддерживается. • В процессе применения политики.
Параметры мобильного устройства не соответствуют политике	Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия.	• Переключатель выключен. • Переключатель включен.
Есть необработанные проблемы безопасности	На устройстве есть необработанные проблемы безопасности. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором.	• Переключатель выключен. • Переключатель включен.
Статус устройства определен приложением	Статус устройства определяется управляемым приложением.	• Переключатель выключен. • Переключатель включен.
На устройстве заканчивается дисковое пространство	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *OK*, когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению.	Более чем 0 МБ
Устройство стало неуправляемым	Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	• Переключатель выключен. • Переключатель включен.
Защита выключена	Устройство видимо в сети, но приложение безопасности на устройстве отключено больше указанного времени. В этом случае состояние приложения безопасности *Остановлено* или *Сбой* и отличается от следующих: *Запускается*, *Выполняется* или *Приостановлено*.	Более чем 0 минут.
Приложение безопасности не запущено	Устройство видимо в сети и приложение безопасности установлено на устройстве, но не запущено.	• Переключатель выключен. • Переключатель включен.

Kaspersky SIEM Cloud позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*. При невыполнении заданных условий клиентскому устройству присваивается статус *OK*.

Разным значениям одного условия могут соответствовать разные статусы. Например, по умолчанию при соблюдении условия **Базы устарели** со значением **Более 3 дней** клиентскому устройству присваивается статус *Предупреждение*, а со значением **Более 7 дней** – статус *Критический*.

Когда Kaspersky SIEM Cloud присваивает устройству статус, для некоторых условий (см. столбец "Описание условий") учитывается видимость устройств в сети. Например, если управляемому устройству был присвоен статус *Критический*, так как выполнено условие Базы устарели, а затем для устройства стало видимо в сети, то устройству присваивается статус *OK*.

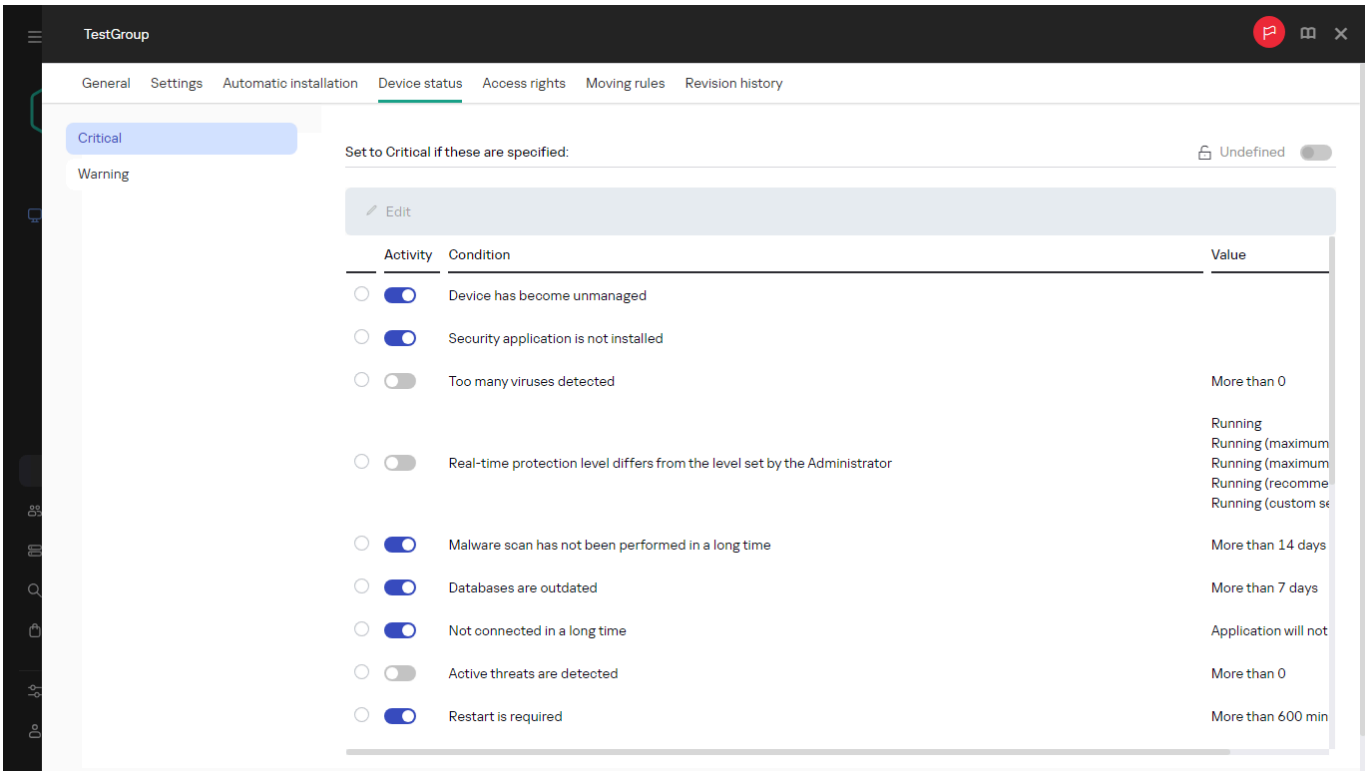
Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

Чтобы изменить статус устройства на Критический:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Иерархия групп**.
2. Перейдите в свойства группы администрирования, для которой вы хотите изменить статусы устройств, одним из следующих способов:
   - Выберите имя группы администрирования.
   - Нажмите на кнопку **Показать иерархию** в верхней части страницы. В открывшейся панели наведите курсор мыши на название нужной группы и нажмите на значок параметров (⚙).

   Откроется окно свойств группы администрирования.
3. В окне свойств выберите вкладку **Статус устройства**.
4. Выберите раздел **Критический**.
5. В блоке **Установить статус "Критический", если** включите условие, чтобы перевести устройство в состояние *Критическое*.



Вы можете изменить только параметры, которые не заблокированы в родительской политике.

6. Установите переключатель рядом с условием в списке.
7. Нажмите на кнопку **Изменить** в верхнем левом углу списка.
8. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.
9. Нажмите на кнопку **OK**.
10. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

При выполнении заданных условий управляемому устройству присваивается статус *Критический*.

Чтобы изменить статус устройства на Предупреждение:

1. В главном окне приложения перейдите в раздел **Управление активами → Иерархия групп**.
2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.
3. В отобразившемся окне свойств выберите вкладку **Статус устройства**.
4. Выберите раздел **Предупреждение**.
5. В блоке **Установить статус "Предупреждение", если**, включите условие, чтобы переключить устройство в состояние *Предупреждение*.

Вы можете изменить только параметры, которые не заблокированы в родительской политике.

6. Установите переключатель рядом с условием в списке.
7. Нажмите на кнопку **Изменить** в верхнем левом углу списка.
8. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.
9. Нажмите на кнопку **OK**.
10. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

При выполнении заданных условий управляемому устройству присваивается статус *Предупреждение*.

Настройка параметров доставки уведомлений

Вы можете настроить уведомления о событиях, возникающих в Kaspersky SIEM Cloud. В зависимости от выбранного способа уведомления доступны следующие типы уведомлений:

- Электронная почта – при возникновении события приложение Kaspersky SIEM Cloud посылает уведомление на указанные адреса электронной почты.
- SMS – при возникновении события приложение Kaspersky SIEM Cloud посылает уведомления на указанные номера телефонов.
- Исполняемый файл – при возникновении события исполняемый файл запускается на Сервере администрирования.

Чтобы настроить параметры доставки уведомлений о событиях, возникших в Kaspersky SIEM Cloud:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.
2. Перейдите в раздел **Уведомление** и на правой панели выберите вкладку с требуемым способом уведомления:

   - **Электронная почта**

     На вкладке **Электронная почта** можно настроить уведомления о событиях по электронной почте.

     В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

     - IPv4-адрес или IPv6-адрес;
     - DNS-имя SMTP-сервера.

     В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если вы включите параметр **Использовать DNS и MX поиск**, вы сможете использовать несколько MX-записей IP-адреса для одного и того же DNS-имени SMTP-сервера. Одно DNS-имя может иметь несколько MX-записей с различными приоритетами полученных электронных писем. Сервер администрирования пытается отправлять уведомления по электронной почте на SMTP-сервер в порядке возрастания приоритета MX-записей.

Если вы включили параметр **Использовать DNS и MX поиск** и не разрешили использование параметров TLS, рекомендуется использовать параметры DNSSEC на вашем серверном устройстве в качестве дополнительной меры защиты при отправке уведомлений по электронной почте.

Если параметр **Использовать ESMTP-аутентификацию** включен, вы можете указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию параметр не выбран и параметры ESMTP-аутентификации недоступны.

Вы можете указать параметры подключения TLS для SMTP-сервера:

- **Не использовать TLS**

Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

- **Использовать TLS, если поддерживается SMTP-сервером**

Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

- **Всегда использовать TLS, для проверки срока действия сертификата сервера**

Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы выбрали значение **Всегда использовать TLS, для проверки срока действия сертификата сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать сертификат для TLS подключения, перейдя по ссылке **Задать сертификаты**:

- Выберите файл сертификата SMTP-сервера:

Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его на Сервер администрирования. Kaspersky SIEM Cloud проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Kaspersky SIEM Cloud не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от доверенного центра сертификации.

- Выберите файл сертификата клиента:

Вы можете использовать сертификат, полученный из любого источника, например, от любого доверенного центра сертификации. Вам нужно указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

- Сертификат X-509:

Вам нужно указать файл с сертификатом и файл с закрытым ключом. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла загружены, необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

- Контейнер pkcs12:

Вам нужно загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

По нажатию на кнопку **Отправить тестовое сообщение** можно проверить правильно ли настроены сообщения: приложение отправляет тестовые сообщения на указанные адреса электронной почты.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой.

В поле **Тема** укажите тему электронной почты, используя подстановочные параметры, например: `[KSC-SAMARA-1] [%SEVERITY%] %EVENT%`. Пример отображения темы письма в случае обнаружения угрозы: `[KSC-SAMARA-1] [Critical] Threat detected`. Также вы можете оставить поле пустым.

В раскрывающемся списке **Тема шаблона** выберите шаблон для темы вашего электронного письма. Переменная, в соответствии с выбранным шаблоном, автоматически отображается в поле **Тема**. Вы можете создать тему электронной почты, выбрав несколько шаблонов темы.

В окне **Адрес электронной почты отправителя: если параметр не задан, будет использоваться адрес получателя. Не рекомендуется указывать в этом поле несуществующий адрес электронной почты** укажите адрес отправителя электронной почты. Если вы оставите поле пустым, по умолчанию используется адрес получателя. Не рекомендуется использовать несуществующий адрес.

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый приложением при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив подстановочные параметры с подробными данными события.

Пример заполнения поля

```
Sender - KSC-SAMARA-1

Host: %COMPUTER%

Product: %KL_PRODUCT%

Version: %KL_VERSION%

Occurred at: %RISE_TIME%

Event: %EVENT%

Details:

%DESCR%
```

Строка `Sender` является необязательной. Например, если у вас несколько Серверов администрирования, вы можете указать в качестве значения имя Сервера администрирования, с которого поступило уведомление: `Sender - KSC-SAMARA-1`.

Пример отображения текста уведомления:

```
Sender - KSC-SAMARA-1
```

```
Host: nb-123456.example.net

Product: Kaspersky Endpoint Security 12.5 for Linux

Version: 12.5.0.1569

Occurred at: 2026-08-17T13:15:36

Event: Threat detected

Details:

Initiator: Product; Task type: ODS; ID of running task: 107; User receiving access:
root; Object type: File; File owner: user; Detection certainty: Sure; File:
/home/user/eicar_com.zip//eicar.com; Detected object name: EICAR-Test-File; Detected
object type: Virware; MD5 hash: <hash>; Unique ID: <ID>
```

> Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

- **SMS**

На вкладке **SMS** можно настроить отправку SMS-уведомлений о различных событиях на мобильный телефон. SMS-сообщения отправляются через почтовый шлюз.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес;
- DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если параметр **Использовать ESMTP-аутентификацию** включен, вы можете указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию параметр не выбран и параметры ESMTP-аутентификации недоступны.

Вы можете указать параметры подключения TLS для SMTP-сервера:

- **Не использовать TLS**

Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

- **Использовать TLS, если поддерживается SMTP-сервером**

Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

- **Всегда использовать TLS, для проверки срока действия сертификата сервера**

Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы выбрали значение **Всегда использовать TLS, для проверки срока действия сертификата сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать файл сертификата SMTP-сервера, перейдя по ссылке **Задать сертификаты**. Вы можете получить файл со списком сертификатов от доверенного центра сертификации и загрузить его на Сервер администрирования. Kaspersky SIEM Cloud проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Kaspersky SIEM Cloud не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от доверенного центра сертификации.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой. Уведомления доставляются на телефоны, номера которых связаны с указанными адресами электронной почты.

В поле **Тема** укажите тему электронной почты.

В раскрывающемся списке **Тема шаблона** выберите шаблон для темы вашего электронного письма. Переменная, в соответствии с выбранным шаблоном, отображается в поле **Тема**. Вы можете создать тему электронной почты, выбрав несколько шаблонов темы.

В окне **Адрес электронной почты отправителя: если параметр не задан, будет использоваться адрес получателя. Не рекомендуется указывать в этом поле несуществующий адрес электронной почты** укажите адрес отправителя электронной почты. Если вы оставите поле пустым, по умолчанию используется адрес получателя. Не рекомендуется использовать несуществующий адрес.

В поле **Номера телефонов получателей SMS-сообщений** укажите номера мобильных телефонов для получения SMS.

В поле **Текст уведомления** напишите текст уведомления о событии, отправляемый приложением при возникновении события. Текст может содержать подстановочные параметры, такие как имя события, имя устройства и имя домена.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Нажмите на кнопку **Отправить тестовое сообщение**, чтобы проверить правильно ли настроены сообщения: приложение отправляет тестовые сообщения указанным получателям.

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

- **Исполняемый файл для запуска**

  Исполняемый файл должен содержать переменные среды события, которые нужно передать администратору.

  В поле **Исполняемый файл, который запустится на Сервере администрирования при возникновении события** укажите папку и имя файла, который запустится.

  Пример заполнения поля:

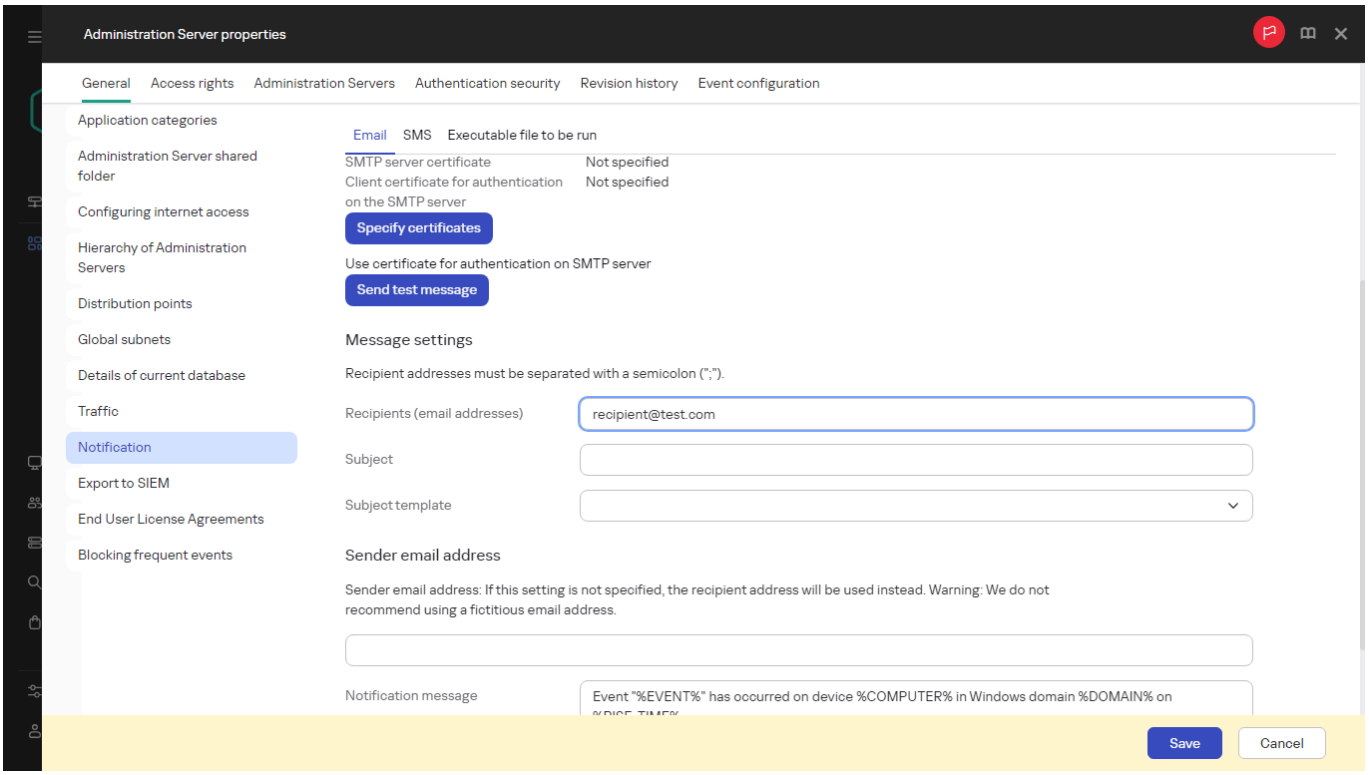
  ```
  /opt/scripts/notifications.sh
  ```

  Файл необходимо подготовить заранее, указав в нем подстановочные параметры, определяющие сведения о событии, которые будут отправлены в сообщении. Папка и файл должны находиться на Сервере администрирования.

  Пример скрипта для тестов или отладки:

```
#!/usr/bin/env bash
touch /tmp/ksc_notification.txt
echo "$RISE_TIME $COMPUTER $EVENT" >> /tmp/ksc_notification.txt
```

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.



Выбор способа уведомления

3. На вкладке настройте параметры уведомлений.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения и закрыть окно свойств Сервера администрирования.

Сохраненные параметры доставки уведомлений применяются ко всем событиям, которые возникают в Kaspersky SIEM Cloud.

Можно изменить значения параметров доставки уведомлений для определенных событий в разделе **Настройка событий** в параметрах Сервера администрирования, параметрах политики или параметрах приложения.

Проверка распространения уведомлений

Для проверки распространения уведомлений о событиях используется уведомление об обнаружении тестового "вируса" Eicar на клиентских устройствах.

Чтобы проверить распространение уведомлений о событиях:

1. Остановите задачу постоянной защиты файловой системы на клиентском устройстве и скопируйте тестовый "вирус" Eicar на клиентское устройство. Затем снова включите задачу постоянной защиты файловой системы.

2. Запустите задачу проверки клиентских устройств для группы администрирования или набора устройств, в который входит клиентское устройство с тестовым "вирусом" Eicar.

   Если задача проверки настроена верно, в процессе ее выполнения тестовый "вирус" будет обнаружен. Если параметры уведомлений настроены верно, вы получите уведомление о найденном вирусе.

Чтобы открыть запись об обнаружении тестового "вируса":

1. В главном окне приложения перейдите в раздел **Мониторинг → Выборки событий**.

2. Нажмите на название выборки **Последние события**.

   В открывшемся окне отображается уведомление о тестовом "вирусе".

Тестовый "вирус" Eicar не содержит программного кода, который может навредить вашему устройству. При этом большинство приложений безопасности компаний-производителей идентифицируют его как вирус. Загрузить тестовый "вирус" можно с официального веб-сайта организации EICAR.

Параметры и переменные среды для описания события

При настройке уведомлений о событиях, возникающих в Kaspersky SIEM Cloud, вы можете использовать для их описания параметры и переменные среды (см. таблицу ниже).

Если в качестве способа уведомления вы выбрали запуск исполняемого файла, используйте переменные при написании файла.

Если вы хотите отправлять уведомления о событиях по электронной почте или SMS, при настройке уведомлений на соответствующей вкладке вы также можете указать переменные в полях **Тема** и **Текст уведомления**.

Параметры и переменные среды для описания события

Параметр подстановки (для использования в уведомлениях)	Переменная среды (для использования в скриптах)	Описание переменной среды
%SEVERITY%	$SEVERITY	Уровень важности события. Возможные значения: • **Информационное сообщение** • **Предупреждение** • **Сбой** • **Критическое**
%COMPUTER%	$COMPUTER	Имя устройства, на котором произошло событие. Максимальная длина имени устройства равна 256 символов.
%DOMAIN%	$DOMAIN	Имя домена устройства, на котором произошло событие.
%EVENT%	$EVENT	Имя типа события. Максимальная длина названия типа события равна 50 символов.

Параметр подстановки (для использования в уведомлениях)	Переменная среды (для использования в скриптах)	Описание переменной среды
%DESCR%	$DESCR	Описание события. Максимальная длина описания равна 1000 символов.
%RISE_TIME%	$RISE_TIME	Время создания события.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	$KLCSAK_EVENT_TASK_DISPLAY_NAME	Название задачи. Максимальная длина названия задачи равна 100 символов.
%KL_PRODUCT%	$KL_PRODUCT	Название приложения.
%KL_VERSION%	$KL_VERSION	Номер версии приложения.
%$KLCSAK_EVENT_SEVERITY_NUM%	$KLCSAK_EVENT_SEVERITY_NUM	Код уровня важности события. Возможные значения: • 1 – **Информационное сообщение**. • 2 – **Предупреждение**. • 3 – **Сбой**. • 4 – **Критическое**.
%HOST_IP%	$HOST_IP	IP-адрес устройства, на котором произошло событие.
%HOST_CONN_IP%	$HOST_CONN_IP	IP-адрес соединения устройства, на котором произошло событие.

Объявления "Лаборатории Касперского"

В этом разделе описано, как использовать, настраивать и отключать объявления "Лаборатории Касперского".

Об объявлениях "Лаборатории Касперского"

Раздел объявлений "Лаборатории Касперского" (**Мониторинг → Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Open Single Management Platform и управляемых приложениях, установленных на управляемых устройствах. Open Single Management Platform периодически обновляет информацию в разделе, удаляет устаревшие объявления и добавляет новую информацию.

Open Single Management Platform показывает только те объявления "Лаборатории Касперского", которые относятся к текущему подключенному Серверу администрирования и приложениям "Лаборатории Касперского", установленным на управляемых устройствах этого Сервера администрирования. Объявления отображаются индивидуально для любого типа Сервера администрирования – главного, подчиненного или виртуального.

Для получения объявлений "Лаборатории Касперского" Сервер администрирования должен иметь подключение к интернету.

Объявления включают информацию следующих типов:

- Объявления, связанные с безопасностью.

Объявления, связанные с безопасностью, предназначены для того, чтобы приложения "Лаборатории Касперского", установленные в вашей сети, были в актуальном состоянии и были полностью функциональными. В объявлениях может содержаться информация о критических обновлениях для приложений "Лаборатории Касперского", исправлениях для обнаруженных уязвимостей и способах устранения других проблем в приложениях "Лаборатории Касперского". По умолчанию объявления, связанные с безопасностью, включены. Если вы не хотите получать объявления, вы можете отключить эту функцию.

Чтобы показать вам информацию, которая соответствует вашей конфигурации защиты сети, Open Single Management Platform отправляет данные на облачные серверы "Лаборатории Касперского" и получает только те объявления, которые относятся к приложениям "Лаборатории Касперского", установленным в вашей сети. Данные, которые могут быть отправлены на серверы, описаны в Лицензионном соглашении, которое вы принимаете при установке Сервера администрирования.

- Рекламные объявления.

  Рекламные объявления включают информацию о специальных предложениях для ваших приложений "Лаборатории Касперского", рекламу и новости "Лаборатории Касперского". Рекламные объявления по умолчанию выключены. Вы получаете этот тип объявлений только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить рекламные объявления, выключив KSN.

  Чтобы показывать вам только актуальную информацию, которая может быть полезна для защиты ваших сетевых устройств и выполнения повседневных задач, Open Single Management Platform отправляет данные на облачные серверы "Лаборатории Касперского" и получает соответствующие объявления. Данные, которые могут быть отправлены на серверы, описан в разделе "Обрабатываемые данные" Положения о KSN.

Информация разделена на следующие категории по важности:

1. Критическая информация.
2. Предупреждение.
3. Информационное сообщение.

При появлении новой информации в разделе Объявления "Лаборатории Касперского" приложение OSMP Console отображает метку уведомления, соответствующую уровню важности объявлений. Вы можете нажать на метку, чтобы просмотреть это объявление в разделе Объявления "Лаборатории Касперского".

Если вы не хотите получать объявления, вы можете отключить эту функцию.

Выключение объявлений "Лаборатории Касперского"

Раздел объявлений "Лаборатории Касперского" (**Мониторинг → Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Open Single Management Platform и управляемых приложениях, установленных на управляемых устройствах. Если вы не хотите получать объявления "Лаборатории Касперского", вы можете отключить эту функцию.

Объявления "Лаборатории Касперского" включают в себя информацию двух типов: объявления, связанные с безопасностью, и рекламные объявления.

Чтобы выключить объявления, связанные с безопасностью:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Объявления "Лаборатории Касперского"**.

3. Переведите переключатель в положение **Объявления, связанные с безопасностью**, выключено.

4. Нажмите на кнопку **Сохранить**.

   Объявления "Лаборатории Касперского" выключены.

Рекламные объявления по умолчанию выключены. Вы получаете рекламные сообщения только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить этот тип объявлений, отключив KSN.

Отключение KSN может повлиять на работу управляемых приложений "Лаборатории Касперского", использующих службы KSN. Эти приложения могут утратить возможность обмена данными о репутации, телеметрией или статистикой с "Лабораторией Касперского".

Получение предупреждения об истечении срока лицензии

Чтобы добавить лицензионный ключ для Kaspersky Endpoint Security для бизнеса Стандартный на Сервер администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** выберите раздел **Лицензионные ключи**.

3. Нажмите на кнопку **Выбрать**.

4. В открывшемся окне выберите ваш файл ключа и нажмите на кнопку **OK**.

   Если лицензионный ключ не отображается, вы можете нажать на кнопку **Добавить лицензионный ключ**, и использовать свой код активации.

Файл ключа будет добавлен в хранилище Сервера администрирования. В этом случае Сервер администрирования генерирует критическое событие *Срок действия лицензии скоро истекает* за один день до истечения срока действия лицензии, а критическое событие *Режим ограниченной функциональности* после истечения срока действия лицензии. Вы можете настроить параметры доставки уведомлений.

Если вы добавляете лицензионный ключ для Kaspersky Endpoint Security для бизнеса Стандартный в хранилище Сервера администрирования, то этот лицензионный ключ считается использованным на одном устройстве.

Cloud Discovery

Kaspersky SIEM Cloud позволяет отслеживать использование облачных сервисов на управляемых устройствах с операционной системой Windows и блокировать доступ к нежелательным облачным сервисам. Cloud Discovery отслеживает попытки пользователей получить доступ к этим службам через браузеры и настольные приложения. Также отслеживает попытки доступа пользователей к облачным сервисам через незашифрованные соединения (например, по протоколу HTTP). Эта функция позволяет выявлять и прекращать скрытое несанкционированное использование облачных сервисов.

Возможность блокировки доступна только в том случае, если вы активировали Kaspersky SIEM Cloud по лицензии Kaspersky Next EDR Optimum или Kaspersky Symphony XDR.

Возможность блокировки доступна только при использовании Kaspersky Endpoint Security 11.2 для Windows и выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.

Можно включить функцию Cloud Discovery и выбрать политики безопасности или профили, для которых ее требуется включить. Можно также включать и выключать функцию отдельно для каждой политики безопасности или профиля. Вы можете заблокировать доступ к облачным сервисам, к которым вы хотите ограничить доступ для пользователей.

Чтобы заблокировать доступ к нежелательным облачным сервисам, убедитесь, что выполнены следующие условия:

- Вы используете версию Kaspersky Endpoint Security 11.2 для Windows или выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.
- Вы приобрели лицензию на Kaspersky, которая дает возможность блокировать доступ к нежелательным облачным сервисам. Подробную информацию см. в справке Kaspersky.

Информация об удачных и заблокированных попытках доступа к облачным сервисам отображается в виджете Cloud Discovery и в отчетах Cloud Discovery. Виджет также показывает уровень риска каждого облачного сервиса. Kaspersky SIEM Cloud получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных профилями безопасности, в которых они включены.

Включение функции Cloud Discovery с помощью виджета

Функция Cloud Discovery получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных политиками безопасности, в которых она включена. Включить или выключить Cloud Discovery можно только для политики Kaspersky Endpoint Security for Windows.

Существуют два способа включить функцию Cloud Discovery:

- С помощью виджета Cloud Discovery.
- В свойствах политики Kaspersky Endpoint Security for Windows.

  Подробную информацию о том, как включить функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security for Windows, см. в разделе Cloud Discovery справки Kaspersky Endpoint Security for Windows.

Обратите внимание, что вы можете выключить функцию Cloud Discovery только в параметрах политики Kaspersky Endpoint Security for Windows.

Чтобы включить Cloud Discovery, у вас должно быть право **Запись** в функциональной области **Общие функции: Базовая функциональность**.

Чтобы включить функцию Cloud Discovery с помощью виджета Cloud Discovery:

1. Откройте Kaspersky SIEM Cloud.
2. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга**.
3. В виджете **Cloud Discovery** нажмите на кнопку **Включить**.

   Если у вас установлен Kaspersky Endpoint Security for Windows версии 12.4, включите функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security for Windows. Подробнее см. раздел Cloud Discovery справки Kaspersky Endpoint Security for Windows.

   Если у вас версия Kaspersky Endpoint Security for Windows ниже версии 12.4, обновите плагин Kaspersky Endpoint Security for Windows до версии 12.5.

4. В открывшемся окне **Включить Cloud Discovery** выберите политики безопасности, для которых вы хотите включить функцию и нажмите на кнопку **Включить**.

   Следующие параметры политики будут включены автоматически: **Внедрение скрипта в веб-трафик для взаимодействия с веб-страницами**, **Мониторинг веб-сеансов** и **Проверка зашифрованных подключений**.

Функция Cloud Discovery включена, виджет добавлен в панель мониторинга.

Добавление виджета Cloud Discovery в панель мониторинга

Вы можете добавить виджет **Cloud Discovery** в панель мониторинга, чтобы отслеживать использование облачных сервисов на управляемых устройствах.

Чтобы добавить виджет Cloud Discovery в панель мониторинга, у вас должно быть право **Запись** в функциональной области **Общие функции: Базовая функциональность**.

Чтобы добавить виджет Cloud Discovery в панель мониторинга:

1. Откройте Kaspersky SIEM Cloud.
2. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга**.
3. Нажмите на кнопку **Добавить или восстановить виджет**.
4. В списке доступных виджетов нажмите на значок шеврона (>) рядом с категорией **Другое**.
5. Выберите виджет **Cloud Discovery** и нажмите на кнопку **Добавить**.

   Если функция Cloud Discovery выключена, следуйте инструкциям в разделе Включение функции Cloud Discovery с помощью виджета.

Выбранный виджет будет добавлен в конец панели мониторинга.

Просмотр информации об использовании облачных сервисов

Виджет **Cloud Discovery** показывает информацию о попытках доступа к облачным сервисам. Виджет также показывает уровень риска каждого облачного сервиса. Kaspersky SIEM Cloud получает информацию об использовании облачных сервисов со всех управляемых устройств, защищенных только теми профилями безопасности, в которых включена эта функция.

Перед просмотром убедитесь, что:

- Виджет Cloud Discovery добавлен в панель мониторинга.
- Функция Cloud Discovery включена.
- У вас есть право **Чтение** в функциональной области **Общие функции: Базовая функциональность**.

Чтобы посмотреть виджет Cloud Discovery:

1. Откройте Kaspersky SIEM Cloud.
2. В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга**.

   Виджет **Cloud Discovery** отображается в панели мониторинга.
3. В левой части виджета **Cloud Discovery** выберите категорию облачных сервисов.

   В таблице в правой части виджета отображается до пяти сервисов из выбранной категории, к которым пользователи чаще всего пытаются получить доступ. Учитываются как успешные, так и заблокированные попытки доступа.
4. В правой части виджета выберите требуемый сервис.

   В таблице ниже отображается до десяти устройств, наиболее часто обращающихся к этому сервису. В этой таблице вы можете сформировать два типа отчетов: отчет об успешных попытках доступа и отчет о заблокированных попытках доступа.

   Также в этой таблице вы можете заблокировать доступ к облачной службе для определенного устройства.

В виджете отображаются запрашиваемые данные.

В отображаемом виджете можно выполнить следующие действия:

- Перейдите в раздел **Мониторинг** → **Отчеты**, чтобы просмотреть отчеты Cloud Discovery.
- Заблокируйте или разрешите доступ к выбранному облачному сервису.

Возможность блокировки доступна только в том случае, если вы активировали Kaspersky SIEM Cloud по лицензии Kaspersky Next EDR Optimum или Kaspersky Symphony XDR.
Возможность блокировки доступна только при использовании Kaspersky Endpoint Security 11.2 для Windows и выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.

Уровень риска облачных сервисов

Cloud Discovery определяет уровень риска для каждого облачного сервиса. Уровень риска помогает определить сервисы, не соответствующие требованиям безопасности вашей организации. Например, вы можете принять во внимание уровень риска при принятии решения о блокировке доступа к определенному сервису.

Уровень риска является оценочным показателем и ничего не говорит о качестве облачного сервиса или о производителе. Уровень риска – это рекомендация экспертов "Лаборатории Касперского".

Уровни риска облачных сервисов отображаются в виджете Cloud Discovery и в списке всех контролируемых облачных сервисов.

Блокировка доступа к нежелательным облачным сервисам

Вы можете заблокировать доступ к облачным сервисам, к которым вы хотите ограничить доступ для пользователей. Вы также можете разрешить доступ к облачным сервисам, которые ранее были заблокированы.

Например, уровень риска можно учесть при принятии решения о блокировке доступа к определенному сервису.

Вы можете заблокировать или разрешить доступ к облачным сервисам для политики безопасности или профиля политики.

Существует два способа заблокировать доступ к нежелательным облачным сервисам:

- С помощью виджета Cloud Discovery.

  В этом случае вы можете заблокировать доступ к сервисам по очереди.

- В свойствах политики Kaspersky Endpoint Security for Windows.

  В этом случае вы можете заблокировать доступ к сервисам по очереди или сразу всю категорию.

  Подробную информацию о том, как включить функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security for Windows, см. в разделе Cloud Discovery справки Kaspersky Endpoint Security for Windows.

Чтобы заблокировать или разрешить доступ к облачному сервису с помощью виджета:

1. Откройте виджет Cloud Discovery и выберите требуемый облачный сервис.
2. В панели **Топ 10 устройств, использующих эту службу** найдите политику безопасности или профиль политики, для которых вы хотите заблокировать или разрешить службу.
3. В соответствующей строке в столбце **Статус доступа в политике или профиле политики** выполните одно из следующих действий:
   - Чтобы заблокировать службу, в раскрывающемся списке выберите **Заблокировано**.
   - Чтобы разрешить службу, в раскрывающемся списке выберите **Разрешено**.
4. Нажмите на кнопку **Сохранить**.

Доступ к выбранной службе заблокирован или разрешен для политики безопасности или профиля политики.

Активные угрозы

Информация о необработанных файлах, обнаруженных на клиентских устройствах, содержится в разделе **Хранилища**, во вложенном разделе **Активные угрозы**.

Отложенная обработка и дезинфекция выполняются приложением безопасности по запросу или после определенного события. Вы можете настраивать параметры отложенного лечения файлов.

Дезинфекция необработанного файла

Чтобы запустить лечение необработанного файла:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Активные угрозы**.
2. Выполните одно из следующих действий:
   - Установите флажок напротив файла, который вы хотите лечить.
   - Выберите название файла, который нужно лечить.
3. Начните лечение файла, нажав на кнопку **Лечить**.

В результате выполняется попытка лечения выбранного файла.

Если файл вылечен, приложение безопасности, установленное на клиентском устройстве, восстанавливает его в исходную папку. Запись о файле удаляется из списка папки **Активные угрозы**. Если лечение файла невозможно, приложение безопасности, установленное на устройстве, удаляет файл с устройства. Запись о файле удаляется из списка папки **Активные угрозы**.

Возможности лечения и удаления файлов могут различаться в зависимости от установленного приложения безопасности, его версии и параметров.

Скачивание необработанного файла

Open Single Management Platform позволяет скачать копии необработанных файлов, обнаруженные на клиентских устройствах. Это относится к файлам, которые обрабатываются или удаляются приложением. Файлы скачиваются на устройство с установленным Open Single Management Platform в указанную папку.

Вы можете скачать копии файлов, если файлы были удалены или изменены во время лечения, а их копии хранятся в хранилище Kaspersky Endpoint Security for Linux на управляемом устройстве.

Чтобы скачать копию необработанного файла:

1. В главном окне приложения перейдите в раздел **Хранилища** → **Активные угрозы**.
2. Выполните одно из следующих действий:
   - Установите флажок напротив файла, который вы хотите скачать.
   - Выберите название файла, который нужно скачать.
3. Начните загрузку, нажав на кнопку **Скачать**.

В результате приложение безопасности клиентского устройства, на котором обнаружен выбранный необработанный файл, скачает копию этого файла в указанную папку.

Удаление файлов из раздела Активные угрозы

*Чтобы удалить файл из раздела **Активные угрозы**:*

1. В главном окне приложения перейдите в раздел **Хранилища** → **Активные угрозы**.
2. Выполните одно из следующих действий:
   - Установите флажок напротив файла, который вы хотите удалить.
   - Выберите название файла, который нужно удалить.
3. Удалите файлы, нажав на кнопку **Удалить**.
4. В открывшемся окне нажмите на кнопку **Удалить**.

В результате приложения безопасности, поместившие выбранные файлы в хранилища на клиентских устройствах, удаляют файлы из этих хранилищ. Записи о файлах удаляются из списка в папке **Активные угрозы**.

Работа с ревизиями объектов

Этот раздел содержит информацию о работе с ревизиями объектов.

Ревизия – это состояние объекта в определенный момент. Каждый раз, когда вы создаете или изменяете объект, создается новая ревизия этого объекта. Каждая ревизия содержит значения всех параметров объекта, актуальных на момент создания или сохранения ревизии.

Объекты, которые поддерживают работу с ревизиями:

- свойства Сервера администрирования;
- политики;
- задачи;
- группы администрирования;
- учетные записи пользователей;
- инсталляционные пакеты.

Вы можете выполнять с ревизиями объектов следующие действия:

- просматривать выбранную ревизию (доступно только для политик);
- откатывать изменения объекта к выбранной ревизии;
- сохранять ревизии в виде файла JSON (доступно только для политик).

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- **Ревизия** – номер ревизии объекта.
- **Время** – дата и время изменения объекта.
- **Пользователь** – имя пользователя, изменившего объект.
- **IP-адрес устройства пользователя** – IP-адрес устройства, с которого был изменен объект.
- **IP-адрес Web Console** – IP-адрес OSMP Console, с помощью которого был изменен объект.
- **Действие** – выполненное действие с объектом.
- **Описание** – описание ревизии изменения параметров объекта.

  По умолчанию описание ревизии объекта не заполнено. Чтобы добавить описание ревизии, выберите нужную ревизию и нажмите на кнопку **Изменить описание**. В открывшемся окне введите текст описания ревизии.

Просмотр и сохранение ревизии политики

Ревизия политики – это сохраненное состояние политики, которое автоматически фиксируется каждый раз при ее изменении и сохранении. Ревизия сдержит параметры политики, профили и правила их активации, метаданные о дате, а также пользователе и IP-адресе, которые создали эту ревизию. Open Single Management Platform позволяет просматривать ревизию политики, чтобы отслеживать изменения настроек, а также сохранять ревизию в файл JSON.

Просмотр и сохранение ревизии политики доступны, если соответствующий веб-плагин управления поддерживает эту функцию.
Опции доступны для политик Сервера администрирования, Агента администрирования, Kaspersky Endpoint Security for Windows (начиная с версии веб-плагина 14.0), Kaspersky Endpoint Security for Linux (начиная с версии веб-плагина 12.4) и Kaspersky Endpoint Security for Mac (начиная с версии веб-плагина 12.2.1 Patch A).

Чтобы просмотреть ревизию политики:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на ревизию политики, которую вы хотите просмотреть и перейдите в раздел **История ревизий**.
3. В списке ревизий политики нажмите на номер ревизии, которую вы хотите просмотреть.

   В открывшемся отчете доступна информация о параметрах политики, ее профилях и правилах активации для них.

   Если размер ревизии превышает 10 МБ, просмотреть ее с помощью OSMP Console невозможно. Вам будет предложено сохранить выбранную ревизию в файл JSON.

   Если размер ревизии не превышает 10 МБ, отображается отчет в формате HTML с параметрами выбранной ревизии политики. Так как отчет отображается во всплывающем окне, убедитесь, что в вашем браузере разрешены всплывающие окна.

В случае политик Kaspersky Endpoint Security for Windows и Kaspersky Endpoint Security for Mac в отчете не будет информации о профилях политик.

Чтобы сохранить ревизию политики в файл JSON,

В списке ревизий политики выберите ревизию, которую вы хотите сохранить и нажмите на кнопку **Сохранить в файл**.

Ревизия сохранена в файле JSON.

При необходимости вы можете сравнить ревизии политики.

Сравнение ревизий политики

Вы можете сравнить предыдущие ревизии политики с ее текущей ревизией, сравнить различные ревизии, выбранные в списке, или сравнить ревизию одной политики с ревизией другой политики. Параметры доступны для политик Сервера администрирования, Агента администрирования, Kaspersky Endpoint Security for Windows (начиная с версии веб-плагина 14.0) и Kaspersky Endpoint Security for Mac (начиная с версии веб-плагина 12.2.1 Patch A).

Сравнение ревизий политик доступно, если соответствующие веб-плагины управления поддерживает эту функцию.

Чтобы просмотреть ревизию политики:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Политики**.
2. Нажмите на политику, ревизии которой вы хотите сравнить.

   Откроется окно свойств политики.
3. Перейдите на вкладку **История ревизий** и установите флажки рядом с ревизиями, которые нужно сравнить.
4. В панели инструментов нажмите на кнопку **Сравнить** и в раскрывающемся списке выберите один из следующих вариантов:

   - **С текущей ревизией**, если вы хотите сравнить ревизию, выбранную на шаге 3, с последней сохраненной ревизией той же политики.
   - **Выбранные ревизии**, если вы хотите сравнить две ревизии, около которых вы установили флажки на шаге 3.

     Порядок установки флажков не влияет на результаты сравнения. По умолчанию более ранняя выбранная ревизия сравнивается с последней ревизией. Например, если вы установите флажки рядом с ревизиями 5 и 1, ревизия 1 будет сравниваться с ревизией 5. Отчет будет содержать информацию о параметрах ревизии 1, которые были добавлены, удалены или изменены по сравнению с ревизией 5.
   - **С ревизией другой политики**, если вы хотите сравнить ревизии двух разных политик.

В открывшейся панели выполните следующие действия:

a. В поле **Название приложения** выберите политику ревизии которой вы хотите сравнить: Агент администрирования или Сервер администрирования.

b. В поле **Название политики** укажите название политики, ревизию которой вы хотите сравнить с той, которую вы выбрали на шаге 3.

Отобразится список ревизий политики.

c. Выберите нужную ревизию и нажмите на кнопку **Сравнить**.

Отчет сравнения ревизий отобразится в формате HTML на новой вкладке вашего браузера.

Если результат сравнения превышает 10 МБ, отобразится соответствующее диалоговое окно. Вы можете нажать на кнопку **Сохранить в файл**, чтобы сохранить отчет в виде файла, или отменить операцию.

Отчет отображается на языке интерфейса вашей OSMP Console. Вы можете развернуть некоторые разделы отчета, нажав на значок стрелки вниз (▼) рядом с разделом или свернуть раздел, нажав на значок стрелки вверх (▲).

Отчет содержит следующую информацию:

- Логотип "Лаборатория Касперского".
- Название отчета.
- Время и дата создания отчета.
- Имя политики, Сервер администрирования и группа администрирования, в которую входит политика (политики), ревизии которой сравнивались.
- Кнопка **Сохранить как HTML**. Если вы нажмете на кнопку, отчет будет сохранен на вашем устройстве.
- Раздел **Сводная информация**, в котором отображается общая информация о сравниваемых ревизиях: имя политики (политик), номер ревизии, время и дата, когда ревизия была сохранена, пользователь, который сохранил ревизию, и описание ревизии.

  Для унаследованных политик пользователь не отображается.

- Различия сравниваемых ревизий. Различия отображаются в следующих разделах:
  - **Добавленные параметры.**
  - **Удаленные параметры.**
  - **Измененные параметры.**
  - **Параметры доступны только для объекта 1** (если вы сравнивали ревизии двух разных политик).
  - **Параметры доступны только для объекта 2** (если вы сравнивали ревизии двух разных политик).

Раздел не отображается, если в нем нет данных.

Откат изменений объекта к предыдущей ревизии

В случае необходимости вы можете откатить изменения объекта. Например, вам может понадобиться вернуть параметры политики к состоянию на определенную дату.

Чтобы откатить изменения объекта:

1. В окне свойств объекта перейдите на вкладку **История ревизий**.
2. В списке ревизий объекта выберите ревизию, к которой нужно откатить изменения.
3. Нажмите на кнопку **Откатить**.
4. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

Произойдет откат к выбранной ревизии. В списке ревизий объекта отобразится запись о выполненном действии. В описании ревизии отобразится информация о номере ревизии, к которой вы вернули объект.

Операция отката доступна только для политик и задач.

Использование Kaspersky SIEM Cloud

Обнаружение угроз

Kaspersky SIEM Cloud использует алерты и инциденты в качестве рабочих элементов, которые должны обрабатываться аналитиками.

Разделы **Алерты** и **Инциденты** отображаются в главном меню, если выполняются следующие условия:

- У вас есть лицензионный ключ для использования Kaspersky SIEM Cloud.
- Вы подключены к корневому Серверу администрирования в Консоли OSMP.
- У вас есть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Подтверждающий, Аудитор.

Работа с алертами

Этот раздел содержит общую информацию об алертах, их свойствах, типичном жизненном цикле и связи с инцидентами. Предоставленные инструкции помогут вам проанализировать таблицу алертов, изменить свойства алертов в соответствии с текущим состоянием жизненного цикла и объединить алерты в инциденты путем связывания или удаления связи алертов.

Раздел **Алерты** отображается в главном меню, если выполняются следующие условия:

- У вас есть лицензионный ключ для использования Kaspersky SIEM Cloud.
- Вы подключены к корневому Серверу администрирования в Консоли OSMP.
- У вас есть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Подтверждающий, Аудитор.

Об алертах

Алерт – это событие в ИТ-инфраструктуре организации, которое было отмечено Kaspersky SIEM Cloud как необычное или подозрительное и которое может представлять угрозу безопасности ИТ-инфраструктуры организации.

Kaspersky SIEM Cloud формирует алерт, когда EPP-приложение (например, Kaspersky Endpoint Security for Windows) обнаруживает в инфраструктуре определенную активность, соответствующую условиям, заданным в правилах обнаружения.

Алерт создается в течение 5 секунд после возникновения события корреляции Kaspersky SIEM Cloud. Если вы ранее настраивали шаблоны уведомлений, вы получите письмо с соответствующим уведомлением по электронной почте.

Также вы можете создать алерт вручную из набора событий.

После детектирования Kaspersky SIEM Cloud добавляет алерты в таблицу алертов как объекты, которые должны быть обработаны аналитиками. Вы не можете удалить алерты. Их можно только закрыть.

Инциденты можно назначить только аналитикам, имеющим право на чтение и изменение алертов и инцидентов.

Вы можете управлять алертами как объектами, используя следующие свойства алертов:

Статус алерта

Возможные значения: **Новый**, **В обработке**, **Закрыт** или **В инциденте**.

Статус алерта показывает текущий статус алерта в его жизненном цикле. Вы можете изменить статус по своему усмотрению, за исключением следующих случаев:

- Вы не можете вернуть закрытые алерты в статус **В обработке**. Закрытые алерты можно вернуть только в статус *Новый*, а затем статус можно изменить на **В обработке**.
- Вы не можете установить статус **В инциденте** вручную. Алерты получают этот статус, когда они связаны с инцидентом.
- Вы можете установить статус **Закрыт** только для связанного алерта. Чтобы установить статус **Новый** или **В обработке**, необходимо отменить связь между алертом и инцидентом.

Уровень критичности алерта

Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критичный**.

Уровень важности алерта показывает, какое влияние этот алерт может оказать на безопасность устройства или корпоративную локальную сеть на основе опыта "Лаборатории Касперского". Уровень важности определяется автоматически и не может быть изменен вручную.

Ответственный за алерт

Владелец алерта, аналитик, который отвечает за расследование алерта. Вы можете изменить ответственного за алерт в любое время. Невозможно изменить исполнителя закрытых алертов.

Вы можете комбинировать и связывать алерты с более крупными рабочими объектами, называемыми *инцидентами*. Вы можете связать алерты с инцидентами вручную или включить правила для автоматического создания инцидентов и связывания алертов. Используя инциденты, аналитики могут исследовать несколько алертов как одну проблему. Когда вы связываете алерт, ни с чем не связанный в текущий момент, с инцидентом, алерт приобретает статус **В инциденте**. Вы можете связать алерт, ни с чем не связанный в текущий момент, с другим инцидентом. В этом случае статус алерта **В инциденте** сохраняется. Вы можете связать с инцидентом не более 200 алертов.

Каждый алерт содержит *детали алерта*, которые содержат всю информацию, относящуюся к алерту. Вы можете использовать эту информацию для исследования алерта, отслеживания событий, предшествующих алерту, просмотра обнаруженных артефактов, затронутых активов или для привязки алерта к инциденту.

Модель данных алерта

Структура алерта представлена полями, которые содержат значения (см. таблицу ниже). Некоторые поля являются объектами или массивами объектов со своим набором полей (например, поля `Assignee` и `Assets`).

Алерт

Поле	Тип значения	Требуется	Описание
`InternalID`	Строка	Да	Внутренний идентификатор алерта (в формате UUID). Значение поля может совпадать со значением `SourceID`.
`ID`	Целое число	Да	Короткий внутренний идентификатор алерта.
`TenantID`	Строка	Да	Идентификатор тенанта, с которым связан алерт (в формате UUID).
`CreatedAt`	Строка	Да	Дата и время создания алерта (в формате RFC 3339).
`UpdatedAt`	Строка	Да	Дата и время последнего изменения алерта (в формате RFC 3339).
`StatusChangedAt`	Строка	Нет	Дата и время последнего изменения статуса алерта (в формате RFC 3339).
`Severity`	Строка	Да	Важность алерта. Возможные значения: • `critical` • `high` • `medium` • `low`
`IntegrationID`	Строка	Да	Идентификатор плагина управления приложения "Лаборатории Касперского", интегрированного в OSMP.
`IntegrationCompatibilityVersion`	Строка	Да	Версия плагина управления приложения "Лаборатории Касперского", интегрированного в OSMP.
`SourceID`	Строка	Нет	Уникальный идентификатор алерта в интегрированном компоненте.
`SourceCreatedAt`	Строка	Нет	Дата и время создания алерта в интегрированном компоненте (в формате RFC 3339).
`FirstEventTime`	Строка	Да	Дата и время первого события телеметрии, связанного с алертом (в формате RFC 3339).
`LastEventTime`	Строка	Да	Дата и время последнего события телеметрии, связанного с алертом (в формате RFC 3339).
`DetectSource`	Строка	Нет	Компонент, который обнаруживает и генерирует алерт.
`DetectionTechnologies`	Массив строк	Нет	Технология срабатывания детектирования.
`Состояние`	Строка	Да	Статус алерта. Возможные значения: • `new` • `inProgress` • `inIncident` • `closed`
`StatusResolution`	Строка	Нет	Решение статуса алерта. Возможные значения: • `truePositive` • `falsePositive` • `lowPriority` • `merged`
`IncidentID`	Строка	Нет	Внутренний идентификатор инцидента, связанного с алертом.
`IncidentLinkType`	Строка	Нет	Способ добавления алерта в инцидент. Возможные значения: • `manual` • `auto`
`Assignee`	Объект `Assignee`	Нет	Оператор, которому назначен алерт.

`MITRETactics`	Массив объектов `MITRETactic`	Нет	Тактики MITRE, связанные со всеми сработавшими IOA-правилами в алерте.
`MITRETechniques`	Массив объектов `MITRETechnique`	Нет	Техники MITRE, связанные со всеми сработавшими IOA-правилами в алерте.
`Observables`	Массив объектов `Observable`	Нет	Наблюдаемые объекты, связанные с алертом.
`Assets`	Массив объектов `Asset`	Нет	Активы, затронутые алертом.
`Rules`	Массив объектов `Rule`	Нет	Сработавшие правила корреляции, на основании которых формируется алерт.
`OriginalEvents`	Массив объектов	Нет	События, на основании которых формируется алерт.
`ExternalRef`	Строка	Да	Ссылка на объект во внешней системе (например, ссылка на инцидент Jira).
`Extra`	Объект	Нет	Данные, связанные с алертом, в формате JSON. Эти данные получены от управляемых приложений "Лаборатории Касперского", когда события преобразуются в алерты. Это поле не используется в интерфейсе.
`AdditionalData`	Объект	Нет	Дополнительная информация об алерте в формате JSON. Эту информацию может заполнить пользователь или плейбук.
`IsCII`	Логический оператор	Да	Индикатор того, что затронутый актив (устройство или учетная запись) является объектом критической инфраструктуры.
`Имя`	Строка	Да	Название алерта.
`Attachments`	Массив объектов `UnkeyedAttachment`	Нет	Вложения, связанные с инцидентом.

Исполнитель

Поле	Тип значения	Требуется	Описание
`ID`	Строка	Да	Идентификатор учетной записи оператора, которому назначен алерт.
`Имя`	Строка	Да	Имя оператора, которому назначен алерт.

MITRETactic

Поле	Тип значения	Требуется	Описание
`ID`	Строка	Да	Идентификатор тактики MITRE, связанной со всеми сработавшими IOA-правилами в алерте.
`Имя`	Строка	Да	Название тактики MITRE, относящейся ко всем сработавшим IOA-правилам в алерте.

MITRETechnique

Поле	Тип значения	Требуется	Описание
`ID`	Строка	Да	Идентификатор техники MITRE, связанной со всеми сработавшими IOA-правилами в алерте.
`Имя`	Строка	Да	Название техники MITRE, относящейся ко всем сработавшим IOA-правилам в алерте.

Наблюдаемый объект

Поле	Тип значения	Требуется	Описание
`Тип.`	Строка	Да	Тип наблюдаемого объекта. Возможные значения: • `ip` • `md5` • `sha256` • `url` • `domain` • `userName` • `hostName`
`Значение`	Строка	Да	Значение наблюдаемого объекта.
`Details`	Строка	Нет	Дополнительная информация о наблюдаемом объекте.

Правило

Поле	Тип значения	Требуется	Описание
`ID`	Строка	Да	Идентификатор сработавшего правила.
`Имя`	Строка	Нет	Имя сработавшего правила.
`Уровень важности`	Строка	Нет	Критичности сработавшего правила. Возможные значения: • `critical` • `high` • `medium` • `low`
`Confidence`	Строка	Нет	Уровень доверия сработавшего правила. Возможные значения: • `high` • `medium` • `low`
`Custom`	Логический оператор	Нет	Индикатор того, что алерт основан на пользовательских правилах.

Актив

Поле	Тип значения	Требуется	Описание
`Тип.`	Строка	Да	Тип затронутого актива (устройство или учетная запись). Возможные значения: • `host` • `user`
`ID`	Строка	Да	Идентификатор затронутого актива (устройства или учетной записи).
`Имя`	Строка	Нет	Имя затронутого устройства, с которым связан алерт (если для параметра `Type` выбрано значение `host`). Имя пользователя затронутой учетной записи, связанной с событиями, на основе которых создается алерт (если для параметра `Type` выбрано значение `user`).

`IsAttacker`	Логический оператор	Нет	Индикатор того, что затронутый актив (устройство или учетная запись) является атакующим.
`IsVictim`	Логический оператор	Нет	Индикатор того, что затронутый актив (устройство или учетная запись) является атакуемым.
`CIICategory`	Строка	Нет	Категория значимости того, что затронутый актив (устройство или учетная запись) является объектом критической инфраструктуры. Возможные значения: • `notCII` • `ciiWithoutCategory` • `ciiFirstCategory` • `ciiSecondCategory` • `ciiThirdCategory`

UnkeyedAttachment

Поле	Тип значения	Требуется	Описание
`AttachmentID`	Строка	Да	Идентификатор вложения (в формате UUID).
`Имя`	Строка	Да	Имя вложения.
`CreatedAt`	Строка	Да	Дата и время создания вложения в формате UTC.
`UpdatedAt`	Строка	Да	Дата и время последнего изменения вложения в формате UTC.
`CreatedBy`	Строка	Да	Индикатор того, что затронутый актив (устройство или учетная запись) является атакуемым.
`Size`	Целое число	Да	Размер вложения, указанный в байтах.
`Состояние`	Строка	Да	Статус вложения, который указывает, находится ли загрузка вложения в процессе, завершена или прервана с ошибкой. Возможные значения: • `completed` • `error` • `uploading`
`Описание`	Строка	Нет	Описание вложения.
`StatusCode`	Строка	Нет	Текст статуса, который отображается пользователю (например, сообщение об ошибке, которое отображается при неудачной попытке загрузки вложения).

Просмотр таблицы алертов

Таблица алертов отображается в разделе **Мониторинг** → **Алерты** и предоставляет обзор всех алертов, зарегистрированных в Kaspersky SIEM Cloud. При необходимости таблицу алертов можно настроить.

Чтобы настроить таблицу алертов, выполните одно из следующих действий:

- Отфильтруйте данные таблицы алертов одним из следующих методов:
  - Использование основного фильтра:

    a. Нажмите на значок фильтра ( ).

    b. На вкладке **Фильтры** укажите и примените критерий фильтрации в открывшемся меню.

- Фильтрация повторно проверенных алертов:

  a. Нажмите на заголовок столбца **Название**.

  b. Установите флажок **Только повторно проверенные алерты** или **Исключить повторно проверенные алерты**.

- Использование контекстного фильтра ячейки для быстрого добавления нового условия фильтра:

  a. Найдите ячейку, содержащую значение, которое требуется добавить в качестве условия фильтра. Обратите внимание, что в ячейках некоторых столбцах нет контекстного фильтра.

  b. Нажмите на значение в ячейке.

  c. В открывшемся списке выберите одно из следующих действий:

  - **Добавить в фильтр**, чтобы добавить значение в условие фильтра.
  - **Исключить из фильтра**, чтобы исключить значение из условий фильтрации.
  - **Копировать**, чтобы скопировать значение в буфер обмена.

- Если вы хотите скрыть или отобразить столбец, нажмите на значок параметров (⚙) и выберите нужный столбец.

Таблица алертов будет настроена и в ней отобразятся требуемые данные.

В таблице алертов есть следующие столбцы:

- **Зарегистрировано**. Дата и время, когда алерт был добавлен в таблицу алертов.
- **Время обновления**. Дата и время последнего изменения в истории алертов.
- **ID алерта**. Уникальный идентификатор алерта.
- **Статус**. Текущий статус алерта.
- **Тип ссылки инцидента**. Способ добавления алерта в инцидент.
- **Важность**. Важность алерта.
- **Название**. Название алерта.
- **Обнаружено**. Одна или несколько категорий обнаруженных объектов. Например, если решение Kaspersky SIEM Cloud обнаружило файл, зараженный вирусом Trojan-Downloader.JS.Cryptoload.ad, в поле **Обнаружено** для этого обнаружения будет указана категория Trojan-Downloader.JS.Cryptoload.ad.
- **Затронутые активы**. Устройства и пользователи, затронутые алертом.

  С момента добавления актива в OSMP требуется приблизительно 2 минуты, пока решение сможет обогащать этим активом события. Например, если вы добавили актив и в течение двух минут произошло корреляционное событие, в созданном алерте такой актив отображаться не будет.

- **Назначен**. Текущий исполнитель алерта.
- **Свойства события**. Артефакты обнаружения, например IP-адреса или MD5-хеши файлов.

- **Подробнее**. Краткая информация об алерте.
- **Статус изменен**. Дата и время последнего изменения статуса алерта.
- **Внешняя ссылка**. Номер алерта во внешней системе.
- **Объект КИИ**. Индикатор наличия связи алерта с активами, относящимися к объектам КИИ.
- **Технология**. Названия модулей или компонентов, сгенерировавших алерт при проверке.

  Возможные значения в этом столбце:

  - IOA
  - SB (Sandbox)
  - IOC
  - KUMA

Особенности агрегации событий в алертах, инициированных правилами IOA

Если Kaspersky SIEM Cloud создал алерт, инициированный правилом IOA, и то же правило IOA срабатывает в результате других событий на этом или других хостах в тот же день, Kaspersky SIEM Cloud агрегирует эти события в одном алерте. Если алерт уже закрыт, Kaspersky SIEM Cloud откроет его повторно. Период агрегации событий заканчивается в 00:00 на следующий день.

Просмотр деталей алерта

Детали алерта – это страница в интерфейсе, которая содержит всю информацию, относящуюся к алерту, включая свойства алерта.

Чтобы просмотреть детали алерта:

1. В главном окне приложения перейдите в раздел **Мониторинг → Алерты**.
2. В таблице алертов нажмите на идентификатор требуемого алерта.

   Отображаются детали алерта.

При необходимости можно обновить информацию в деталях алерта, нажав на кнопку обновления (🔄) рядом с названием алерта.

Панель инструментов в верхней части деталей алерта позволяет выполнять следующие действия:

- Изменять значение поля **Внешняя ссылка**
- Назначить алерт аналитику
- Изменить статус алерта

- Связать алерт с инцидентом
- Отменить связь алерта с инцидентом
- Создать инцидент и привязать к нему алерт

В зависимости от типа алерта сведения об алерте содержат следующие разделы:

- **Сводная информация**

  В зависимости от типа алерта сводная информация может содержать следующие свойства алерта:

  - **Аналитик**. Аналитик, которому назначен алерт.
  - **Имя**. Название алерта. Если название алерта не указано, это поле не отображается.
  - **Тенант**. Имя тенанта, в котором зарегистрирован алерт.
  - **Активы**. Количество учетных записей пользователей и устройств, связанных с алертом.
  - **Важность**. Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критичный**. Уровень важности алерта показывает, какое влияние этот алерт может оказать на безопасность устройства или корпоративную локальную сеть на основе опыта "Лаборатории Касперского".
  - **Правила**. Правила, которые сработали для регистрации алерта. Вы можете нажать на значок с многоточием рядом с названием правила, чтобы открыть контекстное меню. Используйте это меню, чтобы узнать больше о правиле, найти алерты или инциденты, которые были зарегистрированы этим же правилом, или выполнить поиск событий, инициировавших правило, в разделе **Поиск угроз** за период между первым и последним событием алерта.

    Когда в меню вы нажимаете на раздел **Перейти в Поиск угроз**, раздел **Поиск угроз** открывается в той же вкладке. В заголовке раздела отображаются идентификатор и имя алерта, из которого был выполнен переход. Если вы хотите открыть раздел **Поиск угроз** в новой вкладке браузера, зажмите клавишу `Ctrl` и в меню нажмите на раздел **Перейти в Поиск угроз**.

  - **Зарегистрировано**. Дата и время, когда алерт был добавлен в таблицу алертов.
  - **Первое событие**. Дата и время первого события, связанного с алертом.
  - **Последнее событие**. Дата и время последнего события, связанного с алертом.
  - **Внешняя ссылка**. Ссылка на объект во внешней системе (например, ссылка на инцидент Jira). Вы можете нажать на кнопку **Изменить**, чтобы указать внешнюю ссылку. Если алерт был создан из алерта Kaspersky Endpoint Detection and Response alert, ссылка на этот алерт отображается в поле.
  - **Связанный с**. Инцидент, к которому привязан алерт.

- **Тактика MITRE**. Тактика или несколько тактик, зарегистрированных в алерте. Вы можете открыть контекстное меню, нажав на имя тактики MITRE. В контекстном меню можно проводить следующие действия:
  - Чтобы просмотреть подробную информацию о тактике MITRE в Kaspersky TIP, нажмите на кнопку **Найти в Kaspersky TIP**.
  - Чтобы просмотреть подробную информацию о тактике MITRE в базе знаний MITRE ATT&CK, нажмите на кнопку **Найти в MITRE ATTCK**.
  - Скопируйте название тактики MITRE.
- **Техника MITRE**. Техника или несколько техник, зарегистрированных в алерте. Вы можете открыть контекстное меню, нажав на имя техники MITRE. В контекстном меню можно проводить следующие действия:
  - Чтобы просмотреть подробную информацию о технике MITRE в Kaspersky TIP, нажмите на кнопку **Найти в Kaspersky TIP**.
  - Чтобы просмотреть подробную информацию о технике MITRE в базе знаний MITRE ATT&CK, нажмите на кнопку **Найти в MITRE ATTCK**.
  - Скопируйте название техники MITRE.
- **Правила корреляции**. Правила корреляции, сработавшие для обнаружения угрозы и создания алерта.
- **IOA-правила**. IOA-правила, сработавшие для обнаружения угрозы и создания алерта. Вы можете открыть контекстное меню, нажав на имя IOA-правила. В контекстном меню можно проводить следующие действия:
  - Просмотреть подробную информацию о конкретном IOA-правиле, нажав на кнопку **Открыть свойства**.
  - Просмотреть связанные события, нажав на кнопку **Перейти в Поиск угроз**.

    Выполняется перенаправление в раздел **Поиск угроз**, в котором отображаются только события, отслеживаемые данным правилом IOA. По умолчанию события отображаются за 24 часа. В заголовке раздела отображаются идентификатор и имя алерта, из которого был выполнен переход.
  - Найти похожие инциденты.
  - Чтобы просмотреть подробную информацию о IOA-правиле в Kaspersky TIP, нажмите на кнопку **Найти в Kaspersky TIP**.
  - Скопировать имя IOA-правила.
- **Технологии**. Технология обнаружения, используемая для обнаружения угрозы.
- **Источник обнаружения**. Источник, от которого поступил обнаруженный объект. Например, если файл был отправлен в Sandbox для проверки с какого-либо устройства, это устройство является источником обнаружения.
- **Дополнительные данные**. Дополнительная информация об алерте. Вы можете изменить значение в этом поле только с помощью плейбука. Поле отображается, если вы добавили значение.

- **Результат проверки**

  В разделе **Результат проверки** содержится информация о проверяемом файле и результатах проверки, по которым был создан алерт.

- **Результаты IOC-проверки**

  В разделе **Результаты IOC-проверки** приводится информация о правилах IOC, сработавших во время проверки.

  По нажатию на название IOC-правила можно просмотреть подробные сведения об этом IOC-правиле.

  По нажатию на кнопку **Посмотреть отчет** в столбце **Результаты проверки** можно просмотреть подробную информацию о результатах проверки, включая сведения о сети и системе, а также о процессах и файлах, задействованных при проверке.

- **Результаты проверки Cloud Sandbox**

  Раздел **Результаты проверки Kaspersky Sandbox** содержит информацию о результатах обработки объектов в Sandbox, в том числе:

  - Количество обнаруженных объектов и их типы.
  - Количество извлеченных файлов и их типы.
  - Хеши обнаруженных объектов.

  По нажатию на кнопку **Экспорт результатов** можно просмотреть подробную информацию о результатах обработки объектов в операционных системах, доступных в Sandbox, в том числе:

  - Диаграммы статистики обнаружений.
  - Граф дерева активности объектов.
  - Тактики и техники MITRE (см. базу знаний MITRE ATT&CK).
  - Список подозрительных действий в операционной системе.
  - Скриншоты исполнения файла в операционной системе.
  - Системная активность.
  - Сетевая активность.

  Для просмотра всей информации в окне результатов проверки Sandbox можно переключаться между операционными системами и между результатами, полученными **в режиме быстрой проверки** и **в режиме ведения полного журнала**.

- **Проверенные файлы**

  В разделе **Проверенные файлы** приводится информация о проверенных файлах. Для получения дополнительной информации об угрозах, обнаруженных в файлах, на Kaspersky Threat Intelligence Portal, нажмите на название угрозы в столбце **Вердикт**.

- **Подробная информация**

  В разделе **Сведения** можно отслеживать события телеметрии, связанные с алертом.

В таблице событий отображается результат поиска, который вы определяете с помощью SQL-запроса.

Панель инструментов таблицы событий позволяет выполнить следующие действия:

- **Скачать события**. Вы можете нажать на эту кнопку, чтобы загрузить информацию о связанных событиях в CSV-файл (в кодировке UTF-8).

- **Найти в разделе "Поиск угроз"**. Вы можете нажать на эту кнопку и выбрать, какие события хотите просмотреть в разделе **Поиск угроз**.

  Чтобы выполнить поиск по всем событиям:

  1. Нажмите на кнопку **Найти в разделе "Поиск угроз"**.

  2. В зависимости от того, какие события вы хотите отобразить, нажмите на одну из следующих кнопок в раскрывающемся списке:

     - Если хотите отобразить все события, связанные с текущим алертом, нажмите на кнопку **События, связанные с алертом**.

     - Если хотите отобразить все события, на которых сработало связанное с алертом правило IOA, нажмите на кнопку **События, на которых сработало правило IOA**.

     Откроется таблица в разделе **Поиск угроз**, в которой отображаются события, произошедшие в период между первым и последним событием в алерте. В заголовке раздела отображаются идентификатор и имя алерта, из которого был выполнен переход.

  В разделе **Поиск угроз** вы можете запустить поисковый запрос, чтобы найти все события, в которых было задействовано устройство.

  Раздел **Поиск угроз** также позволяет вам вручную связать события с алертами. Это может быть полезно, если вы выясните, что некоторые события относятся к алерту, но не были связаны с алертом автоматически. Дополнительные сведения см. в инструкциях по связыванию или удалению связи событий с алертами.

  Вы можете вернуться к деталям инцидента, нажав на кнопку **Исследование алерта** или нажав на кнопку **Назад** в вашем браузере.

- **Удалить связь с алертом**. Вы можете выбрать событие или несколько событий в таблице и нажать на эту кнопку, чтобы удалить связь выбранных событий с алертом.

- **Активы**

  В окне **Активы** можно выполнить следующие действия:

  - Просмотреть устройства и пользователей, затронутые алертом или вовлеченные в него.

  - Выполните действия по реагированию. Для этого установите флажок рядом с активом, а затем в раскрывающемся списке **Выбрать действие по реагированию** выберите необходимое действие по реагированию.

  - Чтобы экспортировать информацию о затронутых активах в CSV-файл, нажмите на кнопку **Экспортировать в CSV**.

  Таблица активов содержит следующие столбцы:

  - **Тип актива**

    Возможные значения: устройство или пользователь.

- **Имя актива**
- **Идентификатор актива**
- **Имеет признаки**

  Возможные значения: атакующий или атакуемый.
- **Статус авторизации**

  Этот параметр применяется только к типу актива – устройство. Статус авторизации устройства определяется KICS for Networks. Вы можете изменить статус авторизации, применив соответствующее действие по реагированию к устройству.
- **Сервер администрирования**

  Сервер администрирования, который управляет устройством.
- **Группа администрирования**

  Группа администрирования, к которой принадлежит пользователь.
- **Категории**

  Категории активов, в которые входит актив.
- **Отправлено в архив**

  Статус объекта в архиве. Возможные значения: Yes или No.

Нажав на имя пользователя или устройства, вы можете:

- Просмотреть свойства пользователя или устройства.

  Чтобы просмотреть список алертов или инцидентов, связанных с устройством, в окне свойств устройства нажмите на кнопку **Показать связанные** и выберите **Алерты** или **Инциденты**, в зависимости от того что вы хотите просмотреть.
- Скопировать имя пользователя или имя устройства в буфер обмена.
- Выполнить поиск по имени пользователя или идентификатору устройства в других алертах.
- Выполнить поиск по имени пользователя или идентификатору устройства в других инцидентах.
- Выполнить поиск имени пользователя или идентификатора устройства в разделе **Поиск угроз** за период между первым и последним событием алерта.

  Если после нажатия на имя пользователя или название устройства выбрать в меню команду **Перейти в Поиск угроз**, откроется раздел **Поиск угроз** на той же вкладке. В заголовке раздела отображаются идентификатор и имя алерта, из которого был выполнен переход. Если вы хотите открыть раздел **Поиск угроз** в новой вкладке браузера, зажмите клавишу `Ctrl` и в меню нажмите на раздел **Перейти в Поиск угроз**.

Нажав на идентификатор пользователя или идентификатор устройства, вы можете:

- Просмотреть свойства пользователя или устройства.

  Чтобы просмотреть список алертов или инцидентов, связанных с устройством, в окне свойств устройства нажмите на кнопку **Показать связанные** и выберите **Алерты** или **Инциденты**, в зависимости от того что вы хотите просмотреть.

- Скопировать идентификатор пользователя или идентификатор устройства в буфер обмена.
- Выполнить поиск по идентификатору пользователя или идентификатору устройства в других алертах.
- Выполнить поиск по идентификатору пользователя или идентификатору устройства в других инцидентах.
- Выполнить поиск идентификатора пользователя или идентификатора устройства в разделе **Поиск угроз** за период между первым и последним событием алерта.

  Если после нажатия на идентификатор пользователя или идентификатор устройства выбрать в меню команду **Перейти в Поиск угроз**, откроется раздел **Поиск угроз** на той же вкладке. В заголовке раздела отображаются идентификатор и имя алерта, из которого был выполнен переход. Если вы хотите открыть раздел **Поиск угроз** в новой вкладке браузера, зажмите клавишу `Ctrl` и в меню нажмите на раздел **Перейти в Поиск угроз**.

С момента добавления актива в OSMP требуется приблизительно 2 минуты, пока решение сможет обогащать этим активом события. Например, если вы добавили актив и в течение двух минут произошло корреляционное событие, в созданном алерте такой актив отображаться не будет.

- **Файлы**

  Раздел **Файлы** содержит файлы, полученные в результате действий по реагированию или добавленные вручную в этот алерт. Вы можете загружать, скачивать или удалять файлы, связанные с алертом, или изменять описание файлов.

  Вы можете загружать файлы любого расширения. Допускаются дубликаты имен файлов. Максимальное количество файлов, которые вы можете прикрепить к инциденту, и максимальный общий размер файлов, вы можете указать в конфигурационном файле.

  Ограничения по умолчанию:

  - Количество файлов не может превышать 100 на один алерт.
  - Общий размер файла не может превышать 25 МБ на один алерт.

  Чтобы загрузить файлы, нажмите на кнопку **Загрузить** и выберите один или несколько файлов. Если вы попытаетесь загрузить файлы, превышающие ограничения, появится панель **Загрузка файлов** с предупреждающим сообщением. В этой панели вы можете удалять файлы из очереди загрузки до тех пор, пока не исчезнет предупреждающее сообщение, и нажать на кнопку **Загрузить**, чтобы загрузить файлы. Если вы проигнорируете предупреждающее сообщение, загрузка не будет выполнена, а в списке файлов появятся файлы, которые не удалось загрузить, со значком предупреждения рядом с именами файлов.

  После нажатия на кнопку **Загрузить** панель закрывается, и загруженный файл отображается в таблице файлов в сведениях об алерте и в главном меню приложения в разделе **Файлы**. При загрузке большого файла или нескольких файлов вам нужно обновить таблицу, чтобы в ней отображались новые файлы. Если загрузка файла выполняется, в столбце **Имя или полный путь** отображается индикатор загрузки, а в столбце **Размер** отображается размер уже загруженного файла.

Нажмите на файл, чтобы открыть панель **Изменить файл**, на которой отображаются сведения о файле. В этой панели вы можете изменить описание файла.

Используйте флажки для выбора файла или нескольких файлов. Выберите один или несколько файлов и нажмите на кнопку **Скачать**, чтобы скачать архив файлов в формате ZIP. Архив защищен паролем *infected*. Выберите файл или несколько файлов и нажмите на кнопку **Удалить**, чтобы удалить выбранные файлы.

Для загрузки и удаления файлов и изменения описаний файлов требуется право **Запись** в функциональной области **Алерты и инциденты**. Для возможности скачивать файлы требуется право на **Чтение** в функциональной области **Алерты и инциденты**.

- **Наблюдаемые объекты**

  В разделе **Наблюдаемые объекты** вы можете:

  - Просмотреть наблюдаемые объекты, связанные с алертом.
  - Экспортировать информацию о связанных наблюдаемых объектах в CSV-файл, нажав на кнопку **Экспортировать в CSV**.
  - Выполнить поиск в таблице наблюдаемых объектов по данным из столбца **Значение**.

    Для этого в строке поиска начните вводить данные искомого наблюдаемого объекта. При отсутствии совпадений со значениями наблюдаемых объектов из столбца **Значение** отображается пустая таблица.

  Наблюдаемые объекты могут включать:

  - MD5-хеш
  - URL
  - Имя домена
  - SHA256
  - UserName
  - HostName
  - Локальный IP-адрес
  - Удаленный IP-адрес

    Следующие частные IP-адреса не включены в наблюдаемые объекты, связанные с алертом:
    От 10.0.0.0 до 10.255.255.255 с маской подсети 255.0.0.0 или /8.
    От 172.16.0.0 до 172.31.255.255 с маской подсети 255.240.0.0 или /12.
    От 192.168.0.0 до 192.168.255.255 с маской подсети 255.255.0.0 или /16.
    От 100.64.0.0 до 100.127.255.255 с маской подсети 255.192.0.0 или /10.

    Чтобы включить частные IP-адреса в наблюдаемые данные, выполните следующие команды на устройстве администратора:

```
k0s kubectl -n irp set env deploy/transformer -c transformer
OSMP_TRANSFORMER_FILTER_PRIVATE_IPS_DISABLED=true
```

```
k0s kubectl -n irp set env deploy/incident -c incident
OSMP_FILTER_PRIVATE_IPS_DISABLED=true
```

- Локальный порт
- Удаленный порт
- Идентификатор системного процесса
- Уникальный PID
- Полное имя файла

Нажав на ссылку в столбце **Значение**, вы можете:

- Поиск наблюдаемого значения в разделе **Поиск угроз** за период между первым и последним событием алерта.

  Если после перехода по ссылке в столбце **Значение** вы выбираете в меню раздел **Перейти в Поиск угроз**, раздел **Поиск угроз** открывается на той же вкладке. В заголовке раздела отображаются идентификатор и имя алерта, из которого был выполнен переход. Если вы хотите открыть раздел **Поиск угроз** в новой вкладке браузера, зажмите клавишу `Ctrl` и в меню нажмите на раздел **Перейти в Поиск угроз**.

- Выполнить поиск по значению наблюдаемого объекта в других алертах.
- Выполнить поиск по значению наблюдаемого объекта в других инцидентах.
- Скопировать значение наблюдаемого объекта в буфер обмена.

Панель инструментов этого раздела содержит следующие кнопки:

- **Запросить статусы Kaspersky TIP**. Используйте эту кнопку, чтобы получить подробную информацию о выбранном наблюдаемом объекте в Kaspersky Threat Intelligence Portal (Kaspersky TIP). В результате информация обновляется в столбце **Статус обновления**. Требуется интеграция с Kaspersky Threat Intelligence Portal (премиум-доступ).
- **Обогатить данные Kaspersky TIP**. Используйте эту кнопку, чтобы получить подробную информацию обо всех перечисленных наблюдаемых объектах из Kaspersky TIP. В результате информация обновляется в столбце **Обогащение**. Используйте ссылку в столбце **Обогащение**, чтобы открыть полученные сведения об обогащении наблюдаемого объекта. Требуется интеграция с Kaspersky Threat Intelligence Portal (премиум-доступ).

- **Выбор действий по реагированию**. Чтобы выполнить действия по реагированию, установите флажок рядом с наблюдаемым объектом и в выпадающем списке **Выбор действий по реагированию**, выберите необходимые действия по реагированию:

  - **Запустить**. Используйте эту кнопку, чтобы запустить приложение с указанными параметрами.
  - **Получить файл**. Используйте эту кнопку, чтобы скачать архив с файлом на ваше устройство.
  - **Заблокировать (NGFW)**. Используйте эту кнопку, чтобы добавить IP-адрес, URL или домен в список запрещенных на сетевых устройствах.
  - **Управлять службами**. Используйте эту кнопку, чтобы удаленно запускать, останавливать, приостанавливать, возобновлять или удалять службу на устройстве. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.
  - **Прервать процесс**. Используйте эту кнопку, чтобы прервать процессы, связанные с файлом. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.
  - **Удалить файл**. Используйте эту кнопку, чтобы удалять файлы.
  - **Поместить на карантин**. Используйте эту кнопку, чтобы переместить устройство, на котором находится файл, на карантин. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.
  - **Добавить правило запрета**. Используйте эту кнопку, чтобы добавить правило, запрещающее запуск файла. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.
  - **Удалить правило запрета**. Используйте эту кнопку, чтобы удалить правило, запрещающее запуск файла. Эта кнопка доступна только для хешей (MD5 или SHA256) наблюдаемых объектов.

- **Похожие закрытые алерты**

  В разделе **Похожие закрытые алерты** вы можете просмотреть список закрытых алертов, которые имеют те же затронутые артефакты, что и текущий алерт. Затронутые артефакты включают наблюдаемые объекты и затронутые устройства. Похожие закрытые алерты могут помочь вам изучить текущий алерт.

  С помощью списка вы можете оценить степень сходства текущего алерта и других алертов. Сходство рассчитывается следующим образом:

  Сходство = M / T * 100

  Здесь "M" – количество артефактов, совпадающих в текущем и аналогичном алерте, "T" – общее количество артефактов в текущем алерте.

  Если сходство составляет 100%, в текущем алерте нет ничего нового по сравнению с аналогичным алертом. Если сходство равно 0%, текущий и аналогичный алерт полностью различаются. Алерты, имеющие сходство 0%, не включаются в список.

  Расчетное значение округляется до ближайшего целого числа. Если сходство равно значению от 0% до 1%, приложение не округляет это значение до 0%. В этом случае значение отображается меньше 1%.

  При нажатии на идентификатор алерта открываются детали алерта.

Настройка списка похожих закрытых алертов

Вы можете настроить таблицу, используя следующие параметры:

- Отфильтруйте алерты, выбрав период, за который были обновлены алерты. По умолчанию список содержит алерты, которые обновлялись за последние 30 дней.
- Нажмите на значок **Параметры столбцов** (⚙) и выберите, какие столбцы отображать и в каком порядке.
- Нажмите на значок **Фильтр** (▽), выберите и настройте фильтры, которые хотите применить. Если вы выбрали несколько фильтров, они применяются одновременно с помощью логического оператора И.
- Нажмите на заголовок столбца и выберите параметры сортировки. Вы можете отсортировать алерты в порядке возрастания или убывания.

- **Подобные инциденты**

  В разделе **Подобные инциденты** вы можете просмотреть список инцидентов, которые имеют те же затронутые артефакты, что и текущий алерт. Затронутые артефакты включают наблюдаемые объекты и затронутые устройства. Подобные инциденты могут помочь вам решить, может ли текущий алерт быть связан с существующим инцидентом.

  С помощью списка вы можете оценить степень сходства текущего алерта и инцидентов. Сходство рассчитывается следующим образом:

  Сходство = M / T * 100

  Здесь "M" – количество артефактов, совпадающих в текущем и аналогичном инциденте, "T" – общее количество артефактов в текущем алерте.

  Если сходство составляет 100%, в текущем алерте нет ничего нового по сравнению с аналогичным инцидентом. Если сходство равно 0%, текущий алерт и схожий инцидент полностью различаются. Инциденты, имеющие сходство 0%, не включаются в список.

  Расчетное значение округляется до ближайшего целого числа. Если сходство равно значению от 0% до 1%, приложение не округляет это значение до 0%. В этом случае значение отображается меньше 1%.

  При нажатии на идентификатор инцидента открывается подробная информация об инциденте.

Настройка списка похожих инцидентов

Вы можете настроить таблицу, используя следующие параметры:

- Отфильтруйте инциденты, выбрав период, за который были обновлены инциденты. По умолчанию список содержит инциденты, которые обновлялись за последние 30 дней.
- Нажмите на значок **Параметры столбцов** (⚙) и выберите, какие столбцы отображать и в каком порядке.

- Нажмите на значок **Фильтр** (▽), выберите и настройте фильтры, которые хотите применить. Если вы выбрали несколько фильтров, они применяются одновременно с помощью логического оператора И.

- Нажмите на заголовок столбца и выберите параметры сортировки. Вы можете отсортировать инциденты в порядке возрастания или убывания.

- **Комментарии**

  В разделе **Комментарии** вы можете оставлять комментарии, связанные с алертом. Например, вы можете написать комментарий о результатах расследования или при изменении свойств алерта, таких как исполнитель или статус алерта.

  Чтобы сохранить комментарий, нажмите на клавишу **`Enter`**. Чтобы начать новую строку, нажмите на клавиши **`Shift + Enter`**. Чтобы изменить или удалить свой комментарий, используйте кнопки в правом верхнем углу.

  Вы можете редактировать и удалять собственные комментарии только в течение определенного промежутка времени после того, как оставите их. По умолчанию задан период в 15 минут.

  Комментарии других пользователей невозможно изменить или удалить. Для возможности оставлять комментарии требуется право на **Запись** в функциональной области **Алерты и инциденты**.

- **История**

  В разделе **Журнал изменений** вы можете отслеживать изменения, внесенные в алерт как в объект:

  - изменение статуса алерта;
  - изменение исполнителя алерта;
  - связь алерта с инцидентом;
  - удаление связи между алертом и инцидентом;
  - загрузка файла в алерт;
  - удаление файла из алерта.

  В разделе **История реагирований** вы можете просмотреть действия по реагированию, выполненные вручную, а также действия, выполненные в рамках плейбука. Таблица содержит следующие столбцы:

  - **Время**. Время возникновения события.
  - **Запущено**. Имя пользователя, запустившего действие по реагированию.
  - **События**. Описание события.
  - **Параметры реагирования**. Параметры действия по реагированию, указанные в действии по реагированию.
  - **Актив**. Количество активов, для которых было запущено действие по реагированию. Вы можете перейти по ссылке с номером актива, чтобы просмотреть подробную информацию об активе.
  - **Статус действия**. Статус выполнения действия по реагированию. В этом столбце могут

отображаться следующие значения:

- **Ожидание подтверждения** – действие по реагированию ожидает подтверждения для запуска.
- **Запущено** – действие по реагированию выполняется.
- **Успешно** – действие по реагированию завершено без ошибок или предупреждений.
- **Предупреждение** – действие по реагированию завершено с предупреждениями.
- **Ошибка** – действие по реагированию завершено с ошибками.
- **Прервано** – действие по реагированию завершено, так как пользователь прервал выполнение.
- **Истекло время подтверждения** – действие по реагированию завершено, так как время подтверждения для запуска истекло.
- **Отклонено** – действие по реагированию завершено, так как пользователь отклонил запуск.

- **Плейбук**. Название плейбука, в котором было запущено действие по реагированию. Вы можете перейти по ссылке, чтобы просмотреть подробную информацию о плейбуке.
- **Действие по реагированию**. Имя выполненного действия по реагированию.
- **Тип актива.** Тип актива, для которого запускается действие по реагированию. Возможные значения: **Устройство** или **Пользователь**.
- **Активы тенанта**. Тенант, являющийся владельцем актива, для которого было запущено действие по реагированию.

Назначение алертов аналитикам

Как объект, алерт должен быть передан аналитику SOC или группе пользователей для проверки и возможного расследования. Вы можете автоматически назначать алерты аналитикам в выбранной группе пользователей. Подробнее см. раздел Настройка автоматического назначения алертов и инцидентов.

Вы можете изменить исполнителя активного алерта в любое время. Вы не можете изменить исполнителя закрытого алерта.

Алерты можно назначить только аналитикам или группе пользователей, имеющим право на чтение и изменение алертов и инцидентов.

Чтобы назначить алерт или несколько алертов:

1. В главном окне приложения перейдите в раздел **Мониторинг → Алерты**.
2. Установите флажки напротив алертов, которые нужно назначить.

   Вам нужно выбрать только алерты, обнаруженные в одном тенанте. Иначе кнопка **Назначить** будет неактивна.

   Также вы можете назначить алерт аналитику или группе пользователей из деталей алерта. Чтобы открыть детали алерта, перейдите по ссылке с нужным идентификатором алерта.

3. Нажмите на кнопку **Назначить**.

4. В открывшемся окне **Назначить аналитику** выберите пользователя или группу пользователей, которым нужно назначить алерты.

5. Начните вводить имя аналитика или группы пользователей, а затем выберите исполнителя из списка.

   Если вы хотите отменить назначение алертов, выберите **Не назначен**.

   > Вы можете выбрать **Не назначен** для всех алертов, кроме алертов со статусом **Закрыт**.

6. Нажмите на кнопку **Назначить**.

   Алерты назначены.

Также можно назначить алерт с помощью плейбуков.

Изменение статуса алерта

Как объект, алерт имеет статус, который показывает текущий статус алерта в его жизненном цикле.

> Вы можете изменять статусы алертов для своих алертов или алертов других аналитиков, только если у вас есть право доступа для чтения и изменения алертов и инцидентов.

> Если статус алерта изменен вручную, плейбуки не будут запускаться автоматически. Вы можете запустить плейбук для такого алерта вручную.

Алерт может иметь один из следующих статусов:

- **Новое.**

  When Kaspersky SIEM Cloud registers a new alert, the alert has the *New* status. You can change the alert status to *In progress* or *Closed*. When you change the *New* status to *In progress*, the alert is automatically assigned to you. When you change the *New* status to *Closed,* and the alert has no assignee, the alert is automatically assigned to you.

- **В обработке.**

  This status means that an analyst started working on the alert. When you set the *In progress* status, the alert is automatically assigned to you. You can change the *In progress* status to *New* or *Closed*.

- **Закрыто.**

  True positive alerts are to be linked to incidents and be investigated within the incidents. When you close an incident, the linked alerts also gain the *Closed* status. You close an unlinked alert only as false positive or a low-priority alert. When you close an alert, you must select a resolution and provide a short comment.

  The *Closed* status can only be changed to status *New*. If you want to return a closed alert back to active, change its status as follows: *Closed* → *New* → *In progress*.

  When you close an alert linked to an incident, the alert is automatically unlinked from the incident. If the alert that you are going to close has no assignee, the alert is automatically assigned to the analyst who closes the alert.

- **В инциденте.**

  Этот статус назначается алерту при привязке к инциденту. Этот статус нельзя выбрать вручную. Статус *Закрыто* может быть назначен только привязанному алерту. Чтобы сменить этот статус на *Новое* или *В обработке*, необходимо сначала отменить связь алерта с инцидентом.

Чтобы изменить статус одного или нескольких алертов:

1. В главном окне приложения перейдите в раздел **Мониторинг → Алерты**.
2. Выполните одно из следующих действий:
   - Установите флажки напротив алертов, статус которых вы хотите изменить.
   - Перейдите по ссылке с идентификатором алерта, статус которого вы хотите изменить.

     Откроется окно **Детали алерта**.
3. Нажмите на кнопку **Изменить статус**.
4. В панели **Изменить статус** выберите статус, который нужно установить.

   Если вы выбрали статус *Закрыт*, вам нужно выбрать решение.

   > Если вы измените статус алерта на *Закрыт* и этот алерт содержит незавершенные плейбуки или действия по реагированию, все связанные плейбуки и действия по реагированию будут прекращены.

5. Нажмите на кнопку **Сохранить**.

Статусы выбранных алертов будут изменены.

Если алерт добавлен на граф расследования, вы также можете изменить статус алерта на графе.

Также статус алерта можно изменить с помощью плейбуков.

Создание алертов вручную

Вы можете создать алерт вручную из набора событий. Вы можете использовать эту функцию для проверки гипотетического инцидента, который не был обнаружен автоматически.

> Если алерт создан вручную, плейбуки не запускаются автоматически. Вы можете запустить плейбук для такого алерта вручную.

Чтобы создать алерт вручную:

1. В главном окне приложения перейдите в раздел **Мониторинг → Поиск угроз**.
2. Выберите события, для которых вы хотите создать алерт. События должны принадлежать одному тенанту.

3. Нажмите на кнопку **Создать алерт**.

   Откроется окно с созданным алертом, и вы получите соответствующее уведомление по электронной почте, если шаблоны уведомлений настроены. Значение поля **Важность** соответствует максимальной критичности среди выбранных событий.

Алерты, созданные вручную, имеют пустое значение **Правила** в таблице **Мониторинг → Алерты**.

Связь алертов с инцидентами

Вы можете связать один или несколько алертов с инцидентом, по следующим причинам:

- Несколько алертов можно интерпретировать как индикаторы одной и той же проблемы в ИТ-инфраструктуре организации. В этом случае алерты в инциденте можно исследовать как отдельную проблему. Вы можете связать с инцидентом до 200 алертов.
- Один алерт может быть связан с инцидентом, если он определен как истинно положительный.

Вы можете связать алерт с инцидентом, если он имеет любой статус отличный от *Закрыт*. Алерт теряет свой текущий статус и приобретает статус *В инциденте* при связывании с инцидентом. Если вы связываете алерты, которые в настоящее время связаны с другими инцидентами, удаляется связь алертов с текущими инцидентами, так как алерт может быть связан только с одним инцидентом.

> Алерты могут быть связаны только с инцидентом, принадлежащим тому же тенанту.

Алерты могут быть связаны с инцидентом вручную или автоматически.

Связывание алертов вручную

Чтобы связать алерты с существующим или новым инцидентом:

1. В главном окне приложения перейдите в раздел **Мониторинг → Алерты**.
2. Установите флажки рядом с событиями, которые требуется связать с инцидентом.
3. Если вы хотите связать алерты с существующим инцидентом:

   a. Нажмите на кнопку **Связать с инцидентом**.

   b. Выберите инцидент, с которым нужно связать алерты.

   Вы также можете нажать на алерт, чтобы отобразить сведения алерта, и нажать на кнопку **Связать с инцидентом** в панели инструментов.

4. Если вы хотите связать алерты с новым инцидентом:

   a. Нажмите на кнопку **Создать инцидент**.

   b. Заполните свойства нового инцидента: имя, исполнитель, приоритет и описание.

Вы также можете нажать на алерт, чтобы отобразить сведения алерта, и нажать на кнопку **Создать инцидент** в панели инструментов.

5. Нажмите на кнопку **Сохранить**.

Выбранные алерты связаны с существующим или новым инцидентом.

Автоматическая привязка алертов

Если вы хотите, чтобы алерты автоматически связывались с инцидентом, вам нужно настроить правила сегментации.

Удаление связи алертов с инцидентами

Вам может потребоваться удалить связь между алертом и инцидентом, например, если анализ и расследование алертов показали, что алерт не связан с другими алертами в инциденте. При удалении связи алерта с инцидентом Kaspersky SIEM Cloud выполняет следующие действия:

- Обновляет все данные, связанные с инцидентом, чтобы отразить, что алерт больше не относится к инциденту. Например, вы можете просмотреть изменения в деталях инцидента.
- Сбрасывает статус несвязанных алертов на *Новый*.

Чтобы удалить связь алерта с инцидентом:

1. Откройте детали алерта.
2. Нажмите на кнопку **Удалить связь с инцидентом** в панели инструментов.

   Откроется окно **Удалить связь с алертами**.
3. Если вы хотите сменить исполнителя, выберите **Назначить алерты** и укажите нового исполнителя.
4. Если вы хотите добавить комментарий, укажите его в разделе **Комментарий**. Указанный вами комментарий отображается в столбце **Сведения** в разделе **История**.

Для выбранных алертов удалена связь с инцидентом.

Связывание событий с алертами

Если во время расследования вы обнаружили событие, связанное с исследуемым алертом, вы можете связать это событие с алертом вручную.

Вы можете связать событие с алертом, если он имеет любой статус отличный от **Закрыт**.

Чтобы привязать событие к алерту:

1. В главном окне приложения перейдите в раздел **Мониторинг → Алерты**.
2. В списке алертов перейдите по ссылке с идентификатором алерта, с которым вы хотите связать событие.

   Откроется окно **Детали алерта**.
3. Перейдите в раздел **Подробнее** и нажмите на кнопку **Найти в разделе Поиск угроз**.

   Откроется раздел **Поиск угроз**. По умолчанию таблица событий содержит события, связанные с выбранным алертом.

   > Таблица событий содержит только события, связанные с тенантами, к которым у вас есть доступ.
4. В верхней части окна откройте первый раскрывающийся список и выберите **Хранилище**.
5. Откройте третий раскрывающийся список и укажите период.

   Вы можете выбрать предопределенные периоды относительно текущей даты и времени и указать необходимый период, используя поля **Начало периода** и **Окончание периода** или выбрав даты в календаре.
6. Нажмите на кнопку **Выполнить запрос**.
7. В обновленном списке событий выберите событие, которое вы хотите связать с алертом и нажмите на **Связать с алертом**.

Выбранные события привязаны к алерту.

Удаление связи событий с алертами

Вам может потребоваться удалить связь между событием и алертом, например, если анализ и расследование событий показали, что событие не связано с алертами.

Чтобы удалить связь события с алертом:

1. В главном окне приложения перейдите в раздел **Мониторинг → Алерты**.
2. В списке алертов перейдите по ссылке с идентификатором алерта, для которого вы хотите удалить связь с событием.

   Откроется окно **Детали алерта**.
3. В разделе **Подробнее** выберите события, для которых вы хотите удалить связь, а затем нажмите на кнопку **Удалить связь с алертом**.

Для выбранных событий удалена связь с алертом.

Работа с алертами на графе расследования

На графе расследования вы можете выполнять следующие действия с алертами:

- Добавлять алерт на граф.
- Скрывать алерт с графа.
- Просматривать детали алерта, выбрав соответствующий элемент из контекстного меню узла алерта.
- Изменять статус алерта.
- Просматривать события, связанные с алертом.
- Просматривать активы, связанные с алертом.
- Просматривать наблюдаемые объекты, связанные с алертом.

Добавление алертов на граф расследования

Вы можете добавить алерт на граф расследования одним из следующих способов:

- Из общей таблицы алертов, которая открывается при нажатии на кнопку **Добавить алерт** на графе расследования. Вам нужно установить флажки рядом с алертами, которые вы хотите отобразить на графе расследования, и нажать на кнопку **Показать на графе**.
- Из таблицы похожих алертов.

Чтобы добавить алерты на граф расследования из таблицы похожих алертов:

1. Выполните одно из следующих действий:
   - Если на графе расследования у вас есть актив, наблюдаемый объект или правило сегментации, нажмите на его узел, а затем в контекстном меню выберите пункт **Найти похожие алерты**.
   - Если на графе расследования у вас есть событие, нажмите на его узел, а затем в контекстном меню выберите пункт **Просмотреть информацию**. В открывшемся окне нажмите на кнопку **Показать на графе**.
   - Если на графе расследования у вас есть алерт, нажмите на его узел и в контекстном меню выберите пункт **События**. В таблице событий нажмите на событие, детали которого вы хотите открыть. Если детали события содержат наблюдаемый объект, актив или правило сегментации, нажмите на ссылку в соответствующем поле, а затем в контекстном меню выберите пункт **Найти похожие алерты**.
   - На графе расследования нажмите на кнопку **Поиск угроз**, а затем в общей таблице событий нажмите на событие, детали которого вы хотите открыть. Если детали события содержат наблюдаемый объект, актив или правило сегментации, нажмите на ссылку в соответствующем поле, а затем в контекстном меню выберите пункт **Найти похожие алерты**.

Отобразится таблица похожих алертов.

2. Установите флажки рядом с алертами, которые вы хотите отобразить на графе расследования, и нажмите на кнопку **Показать на графе**.

Выбранные алерты будут добавлены на граф расследования.

Скрытие алертов на графе расследования

Вы можете скрыть алерты на графе расследования одним из следующих способов:

- Нажать на узел алерта и в контекстном меню выбрать пункт **Скрыть**.
- С помощью таблицы алертов.

Чтобы скрыть алерты на графе с помощью таблицы алертов:

1. Выполните одно из следующих действий:
   - В панели инструментов в верхней части графа расследования нажмите на кнопку **Добавить алерт**.
   - Если на графе отображаются узлы наблюдаемых объектов, активов или событий, нажмите на узел, для которого вы хотите добавить алерт, а затем в контекстном меню выберите пункт **Найти похожие алерты**.

   Отобразится таблица алертов.

2. Установите флажки рядом с алертами, которые вы хотите скрыть на графе расследования, и нажмите на кнопку **Показать на графе**.

Выбранные алерты и их ссылки будут скрыты на графе расследования. Связанные узлы останутся на графе расследования.

Изменение статуса алерта

Чтобы изменить статус алерта:

1. Нажмите на узел алерта и в контекстном меню выберите пункт **Изменить статус**.
2. В открывшейся панели Смена статуса, выберите статус и нажмите на кнопку **Сохранить**.

   Если вы выбрали статус *Закрыт*, вам нужно выбрать решение.

Статусы выбранных алертов будут изменены.

Просмотр событий, связанных с алертом

Чтобы просмотреть события, связанные с алертом, выполните одно из следующих действий:

- Нажмите на цифру рядом с узлом алерта, события которого вы хотите отобразить. Цифра показывает количество событий, связанных с алертом.
- Нажмите на узел алерта, события которого вы хотите отобразить, и в контекстном меню выберите пункт **События**.

Если вы хотите добавить события из таблицы на граф расследования, установите флажки рядом с событиями и нажмите на кнопку **Показать на графе**.

Если вы хотите скрыть события на графе расследования, установите флажки рядом с событиями и нажмите на кнопку **Скрыть на графе**.

Просмотр активов, связанных с алертом

Чтобы просмотреть активы, связанные с алертом, нажмите на узел алерта.

В контекстном меню цифры рядом с элементами **Устройства** и **Пользователи** показывают количество устройств и пользователей, связанных с алертом.

Если вы хотите добавить устройства или пользователей на граф расследования, выберите соответствующий пункт меню.

Просмотр наблюдаемых объектов, связанных с алертом

Чтобы просмотреть наблюдаемые объекты, связанные с алертом, нажмите на узел алерта и в контекстном меню выберите пункт **События**.

В открывшемся меню цифры рядом с элементами показывают количество наблюдаемых объектов, связанных с алертом.

Если вы хотите добавить наблюдаемый объект (например, **Хеш**, **Домен**, **IP-адрес**) на граф расследования, выберите соответствующий пункт меню.

Рекомендации по обработке отдельных типов алертов

IoA алерты

Работа с инцидентами

This section contains general information about incidents, their properties, typical life cycle, and connection with alerts. This section also gives instructions on how to create incidents, analyze the incident table, change incident properties according to the current state in the life cycle, and merge incidents.

Раздел **Инциденты** отображается в главном меню, если выполняются следующие условия:

- У вас есть лицензионный ключ для использования Kaspersky SIEM Cloud.
- Вы подключены к корневому Серверу администрирования в Консоли OSMP.
- У вас есть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Подтверждающий, Аудитор, Взаимодействие с дочерними инцидентами.

Об инцидентах

Инцидент – это контейнер обнаружений, который обычно указывает на истинно положительную проблему в ИТ-инфраструктуре организации. Инцидент может содержать один или несколько алертов. Используя инциденты, аналитики могут исследовать несколько алертов как одну проблему.

Вы можете создавать инциденты вручную или включить правила автоматического создания инцидентов. После создания инцидента вы можете связать алерты с ним. Вы можете связать с инцидентом до 200 алертов.

После создания инцидентов Kaspersky SIEM Cloud добавляет их в таблицу инцидентов как объекты, которые должны быть обработаны аналитиками.

Инциденты можно назначить только аналитикам, имеющим право на чтение и изменение алертов и инцидентов.

Вы можете управлять инцидентами как объектами, используя следующие свойства инцидента:

- **Статус инцидента.**

  Возможные значения: *Новый*, *В обработке*, *Отложен* или *Закрыт*.

  Статус инцидента показывает текущее состояние инцидента в его жизненном цикле. Вы можете изменить статус по своему усмотрению, за исключением следующих случаев:

  - Статус *Новый* невозможно изменить на статус *Отложен*.
  - Статус *Закрыт* можно изменить только на статус *Новый*.

- **Уровень важности инцидента.**

  Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критичный**.

  Уровень важности инцидента показывает, какое влияние этот инцидент может оказать на безопасность устройства или корпоративную локальную сеть на основе опыта "Лаборатории Касперского". Уровень важности инцидента соответствует наивысшему уровню важности связанных алертов и не может быть изменен вручную.

- **Приоритет инцидента.**

  Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критичный**.

  Приоритет инцидентов определяет порядок, в котором инциденты должны расследоваться аналитиками. Инциденты с приоритетом **Критический** являются наиболее важными и должны быть расследованы в первую очередь. Вы можете изменить приоритет инцидента вручную.

- **Исполнитель инцидента.**

  Владелец инцидента, аналитик, который отвечает за расследование и обработку инцидента. Вы можете изменить исполнителя инцидента в любое время, если параметр **Статус** не равен **Закрыт**.

Два или более инцидента могут быть интерпретированы как индикаторы одной и той же проблемы в ИТ-инфраструктуре организации. В этом случае вы можете объединить инциденты, чтобы исследовать их как единую проблему.

У каждого инцидента есть *свойства инцидента*, которые предоставляют всю информацию, связанную с инцидентом. Вы можете использовать эту информацию для расследования инцидента или объединения инцидентов.

Для каждого инцидента вы можете создавать дочерние инциденты. Дочерние инциденты позволяют вам исследовать инциденты и реагировать на них в разных тенантах. Вы также можете создать дочерний инцидент другого дочернего инцидента. Родительский инцидент может иметь не более 200 дочерних инцидентов.

Модель данных инцидента

Структура инцидента представлена полями, которые содержат значения (см. таблицу ниже). Некоторые поля являются объектами или массивами объектов со своим набором полей (например, поля `Assignee` и `Alerts`).

Инцидент

Поле	Тип значения	Требуется	Описание
`InternalID`	Строка	Да	Внутренний идентификатор инцидента (в формате UUID).
`ID`	Целое число	Да	Короткий внутренний идентификатор инцидента.
`TenantID`	Строка	Да	Идентификатор тенанта, с которым связан инцидент (в формате UUID).
`IncidentType`	Объект `IncidentType`	Да	Тип инцидента.
`Имя`	Строка	Да	Название инцидента.
`WorkflowName`	Строка	Да	Имя рабочего процесса инцидента.
`WorkflowUUID`	Строка	Да	Уникальный идентификатор рабочего процесса инцидента в формате UUID.
`Описание`	Строка	Нет	Описание инцидента.
`CreatedAt`	Строка	Да	Дата и время создания инцидента (в формате RFC 3339).
`UpdatedAt`	Строка	Да	Дата и время последнего изменения инцидента (в формате RFC 3339).
`StatusChangedAt`	Строка	Нет	Дата и время последнего изменения статуса инцидента (в формате RFC 3339).

`Severity`	Строка	Нет	Важность инцидента. Возможные значения: • `critical` • `high` • `medium` • `low`
`Приоритет`	Строка	Да	Приоритет инцидента. Возможные значения: • `critical` • `high` • `medium` • `low`
`Assignee`	Объект `Assignee`	Нет	Оператор, которому назначен инцидент.
`FirstEventTime`	Строка	Нет	Дата и время первого события телеметрии алерта, связанного с инцидентом (в формате RFC 3339).
`LastEventTime`	Строка	Нет	Дата и время последнего события телеметрии алерта, связанного с инцидентом (в формате RFC 3339).
`Состояние`	Строка	Да	Статус инцидента. Возможные значения: • `open` • `inProgress` • `hold` • `closed`
`StatusUUID`	Строка	Да	Идентификатор статуса инцидента (в формате UUID).
`StatusResolution`	Строка	Нет	Решение статуса инцидента. Возможные значения: • `truePositive` • `falsePositive` • `lowPriority` • `merged`
`DetectSources`	Массив строк	Нет	Компоненты, которые обнаруживают и генерируют инцидент.
`DetectionTechnologies`	Массив строк	Нет	Технология срабатывания детектирования.
`Alerts`	Массив объектов `Alert`	Нет	Алерты, включенные в инцидент.
`AdditionalData`	Объект	Нет	Дополнительная информация об алерте в формате JSON. Эту информацию может заполнить пользователь или плейбук.
`ExternalRef`	Строка	Да	Ссылка на объект во внешней системе (например, ссылка на инцидент Jira).
`SignOfCreation`	Строка	Да	Способ создания инцидента.
`IsCII`	Логический оператор	Да	Индикатор того, что затронутый актив (устройство или учетная запись) является объектом критической инфраструктуры.
`Attachments`	Массив объектов `UnkeyedAttachment`	Нет	Вложения, связанные с инцидентом.

IncidentType

Поле	Тип значения	Требуется	Описание
`ID`	Строка	Да	Идентификатор типа инцидента (в формате UUID).
`Имя`	Строка	Да	Имя типа инцидента.
`Описание`	Строка	Да	Описание типа инцидента.

Исполнитель

Поле	Тип значения	Требуется	Описание
`ID`	Строка	Да	Идентификатор учетной записи оператора, которому назначен инцидент.
`Имя`	Строка	Да	Имя оператора, которому назначен инцидент.

UnkeyedAttachment

Поле	Тип значения	Требуется	Описание
`AttachmentID`	Строка	Да	Идентификатор вложения (в формате UUID).
`Имя`	Строка	Да	Имя вложения.
`CreatedAt`	Строка	Да	Дата и время создания вложения в формате UTC.
`UpdatedAt`	Строка	Да	Дата и время последнего изменения вложения в формате UTC.
`CreatedBy`	Строка	Да	Индикатор того, что затронутый актив (устройство или учетная запись) является атакуемым.
`Size`	Целое число	Да	Размер вложения, указанный в байтах.
`Состояние`	Строка	Да	Статус вложения, который указывает, находится ли загрузка вложения в процессе, завершена или прервана с ошибкой. Возможные значения: • `completed` • `error` • `uploading`
`Описание`	Строка	Нет	Описание вложения.
`StatusCode`	Строка	Нет	Текст статуса, который отображается пользователю (например, сообщение об ошибке, которое отображается при неудачной попытке загрузки вложения).

Создание инцидентов

Вы можете создавать инциденты вручную или включить правила автоматического создания инцидентов. В этой статье описано, как создавать инциденты вручную.

Чтобы иметь возможность создавать инциденты, у вас должны быть права на чтение и изменение алертов и инцидентов.

Если инцидент создается вручную, плейбуки не запускаются автоматически. Вы можете запустить плейбук для такого инцидента вручную.

Вы можете создавать инциденты с помощью таблицы инцидентов или таблицы алертов.

Создание инцидентов с помощью таблицы инцидентов

Чтобы создать инцидент:

1. В главном окне приложения перейдите в раздел **Мониторинг → Инциденты**. Нажмите на кнопку **Создать инцидент**.

2. На шаге **Общие параметры** укажите следующие параметры:

   - Название инцидента.

   - **Исполнитель**

     Владелец инцидента, аналитик, который отвечает за расследование и обработку инцидента. Вы можете изменить исполнителя инцидента в любое время, если параметр **Статус** не равен **Закрыт**.

   - **Приоритет**

     Возможные значения: **Низкий**, **Средний**, **Высокий** или **Критичный**.

     Приоритет инцидентов определяет порядок, в котором инциденты должны расследоваться аналитиками. Инциденты с приоритетом **Критический** являются наиболее важными и должны быть расследованы в первую очередь. Вы можете изменить приоритет инцидента вручную.

   - **Описание**

     В этом поле вы можете написать описание инцидента. Например, вы можете описать проблему или предоставить результаты расследования связанных алертов. Описание будет добавлено в раздел **Описание** в сведениях об инциденте.

     Поле не является обязательным.

3. Нажмите на кнопку **OK**.

   Инцидент создан.

Создание инцидентов с помощью таблицы алертов

Вы создаете инцидент, выбирая алерты для связи с новым инцидентом. См. как связать алерты с инцидентами.

Создание дочерних инцидентов

Дочерние инциденты позволяют вам отслеживать ход расследования инцидентов и реагировать на инциденты в разных тенантах. Вы также можете создать дочерний инцидент другого дочернего инцидента. Родительский инцидент может иметь до 200 дочерних инцидентов.

У вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Подтверждающий, Взаимодействие с дочерними инцидентами.

Создать дочерний инцидент:

1. В главном окне приложения перейдите в раздел **Мониторинг → Инциденты**.
2. В таблице инцидентов нажмите на идентификатор требуемого инцидента.

   Откроется окно **Детали инцидента**.
3. В разделе **Дочерние инциденты** нажмите на кнопку **Создать**.

   Откроется окно **Создать дочерний инцидент**.
4. При необходимости в поле **Название** измените название дочернего инцидента.

   По умолчанию название дочернего инцидента включает тег [Child] и название родительского инцидента.
5. В раскрывающемся списке **Тенант** выберите тенант, которому будут назначены дочерние инциденты.
6. В раскрывающемся списке **Аналитик** начните вводить имя аналитика, а затем выберите его имя из списка.

   Вы также можете выбрать вариант **Не назначен**.
7. При необходимости раскрывающемся списке **Приоритет** измените приоритет инцидента.

   По умолчанию дочерний инцидент наследует приоритет от родительского инцидента.
8. При необходимости в поле **Описание** укажите описание дочернего инцидента.
9. Если вы хотите скопировать всю информацию из родительского инцидента, установите флажок **Копировать информацию из родительского инцидента**.

   Если этот флажок установлен, все данные, включая наблюдаемые объекты, активы и связанные алерты, будут скопированы из родительского инцидента. Скопированные алерты будут назначены тенанту дочернего инцидента.

   Если этот флажок снят, дочерний инцидент не будет содержать информацию об активах, наблюдаемых и связанных алертах родительского инцидента.
10. Нажмите на кнопку **Создать**.

Дочерний инцидент создается и связывается с родительским инцидентом. Дочерний инцидент находится в разделе **Дочерние инциденты** окна **Детали инцидента**.

Если родительский инцидент имеет такой тип, которого нет у тенанта назначенному дочернему инциденту, то дочернему инциденту назначается тип инцидента по умолчанию и рабочий процесс инцидента по умолчанию. При необходимости вы можете изменить тип инцидента.

Просмотр таблицы инцидентов

Таблица инцидентов с обзором всех созданных инцидентов отображается в разделе **Мониторинг → Инциденты**. При необходимости таблицу инцидентов можно настроить.

Чтобы настроить таблицу инцидентов, выполните одно из следующих действий:

- Отфильтруйте данные таблицы алертов:

  a. Нажмите на значок фильтра ( ).

  b. На вкладке **Фильтры** укажите и примените критерий фильтрации в открывшемся меню.

- Если вы хотите скрыть или отобразить столбец, нажмите на значок параметров ( ) и выберите нужный столбец.

Таблица инцидентов будет настроена, и в таблице отобразятся требуемые данные.

В таблице инцидентов есть следующие столбцы:

- **Создан**. Дата и время создания инцидента.
- **Продолжительность угрозы**. Время между самыми ранними и самыми последними событиями среди всех алертов, связанных с инцидентом.
- **Время обновления**. Дата и время последнего изменения в истории инцидента.
- **ID инцидента**. Уникальный идентификатор инцидента.
- **Статус**. Текущий статус инцидента.
- **Время на рассмотрение**. Срок рассмотрения инцидента в днях, часах и минутах.
- **Время, использованное на ответ**. Срок первоначального реагирования на инцидент в днях, часах и минутах.
- **Время на разрешение**. Срок разрешения инцидента в днях, часах и минутах.
- **Статус изменен**. Дата и время изменения статуса инцидента.
- **Важность.** Уровень важности инцидента.
- **Приоритет**. Приоритет инцидента.
- **Связан с алертами**. Сколько алертов включено в инцидент.
- **Название**. Название инцидента.
- **Правила**. Правила, которые сработали для создания инцидента.
- **Затронутые активы**. Устройства и пользователи, затронутые инцидентом. Если количество активов, затронутых инцидентом или вовлеченных в него, больше или равно трем, отображается количество затронутых устройств.
- **Внешняя ссылка**. Номер инцидента во внешней системе.
- **Исполнитель**. Текущий исполнитель инцидента.

- **Есть родительский инцидент**. Наличие у инцидента родительского инцидента. Если отображается значение **Да**, инцидент является дочерним инцидентом.
- **Статус дочерних инцидентов**. Результирующий статус дочерних инцидентов первого уровня. Возможные значения: **Закрыто**, **В обработке**, **Дочерних инцидентов нет**.
- **Метод создания**. Как был создан инцидент, вручную или автоматически.
- **Наблюдаемые объекты**. Количество обнаруженных артефактов, например IP-адреса или MD5-хеши файлов. Если количество наблюдаемых объектов — три или больше, отображается количество наблюдаемых объектов.

Если требуется, можно экспортировать информацию обо всех инцидентах, которые отображаются в таблице инцидентов, в файл JSON.

Назначение инцидентов аналитикам

Как объект, инцидент должен быть передан аналитику SOC или группе пользователей для проверки и возможного расследования. Вы можете автоматически назначать инциденты аналитикам в выбранной группе пользователей. Подробнее см. раздел Настройка автоматического назначения алертов и инцидентов.

Вы можете изменить исполнителя инцидента в любое время.

Инциденты можно назначить только аналитикам или группе пользователей, имеющим право на чтение и изменение алертов и инцидентов.

Чтобы назначить инцидент или несколько инцидентов:

1. В главном окне приложения перейдите в раздел **Мониторинг → Инциденты**.
2. Установите флажки напротив инцидентов, которые требуется назначить.

   Вам нужно выбрать только инциденты, обнаруженные в одном тенанте. Иначе кнопки **Назначить мне** и **Назначить** будут неактивны.

   Также вы можете назначить инцидент аналитику или группе пользователей из деталей инцидента. Чтобы открыть детали инцидента, нажмите на ссылку с идентификатором инцидента.
3. Выполните одно из следующих действий:
   - Чтобы назначить инциденты себе, нажмите на кнопку **Назначить мне**.
   - Чтобы назначить инциденты другому аналитику или группе пользователей:
     a. Нажмите на кнопку **Назначить**.
     b. В открывшемся окне **Назначить** выберите пользователя или группу пользователей, которым нужно назначить инциденты.
     c. Начните вводить имя аналитика или группы пользователей, а затем выберите исполнителя из списка.
     d. Нажмите на кнопку **Назначить**.

Если вы хотите отменить назначение инцидентов, выберите **Не назначен**.

Инциденты назначены.

Также назначить аналитика для решения инцидента можно с помощью плейбуков.

Изменение статуса инцидента

Как объект, инцидент имеет статус, который показывает текущее состояние инцидента в его жизненном цикле.

Вы можете изменять статус для своих инцидентов или инцидентов других аналитиков, только если у вас есть право доступа для чтения и изменения алертов и инцидентов.

При изменении статуса инцидент и все неназначенные связанные алерты автоматически назначаются вам.

Если статус инцидента изменен вручную, плейбуки не будут запускаться автоматически. Вы можете запустить плейбук для такого инцидента вручную.

Инцидент может иметь один из следующих статусов:

- **Новый**

  When you create an incident or it is created automatically, the incident has the *New* status. You can change the status to *In progress* or *Closed*. When you change the *New* status to *Closed* and the incident has no assignee, the incident is automatically assigned to you.

- **В обработке**

  This status means that an analyst started working on the alert. When you set the *In progress* status, the alert is automatically assigned to you. You can change the *In progress* status to *New* or *Closed*.

- **Отложен**

  Этот статус назначается алерту при привязке к инциденту. Этот статус нельзя выбрать вручную. Статус *Закрыто* может быть назначен только привязанному алерту. Чтобы сменить этот статус на *Новое* или *В обработке*, необходимо сначала отменить связь алерта с инцидентом.

- **Закрыт**

  Вы закрываете инциденты, когда не требуется никакой дополнительной работы над инцидентом. Вы можете закрыть инцидент, по которому принято одно из следующих решений:

  - Верное срабатывание.
  - Ложное срабатывание.
  - Низкий приоритет.

При закрытии инцидента, связанные обнаружения также получают статус *Закрыто* и наследуют решение инцидента. Если у инцидента нет исполнителя, закрытый инцидент автоматически назначается вам. Если закрытый инцидент имеет неназначенные связанные обнаружения, эти обнаружения автоматически назначаются вам.

Статус *Закрыт* можно изменить только на статус *Новый*. Если вы хотите вернуть закрытый инцидент в работу, измените его статус следующим образом: *Закрыт → Новый → В обработке*.

Чтобы изменить статус одного или нескольких инцидентов:

1. В главном окне приложения перейдите в раздел **Мониторинг → Инциденты**.
2. Выполните одно из следующих действий:
   - Установите флажки напротив инцидентов, которым требуется изменить статус.
   - Перейдите по ссылке с идентификатором инцидента, статус которого вы хотите изменить.

     Откроется окно **Детали инцидента**.
3. Нажмите на кнопку **Изменить статус**.
4. В панели **Изменить статус** выберите статус, который нужно установить.

   Если выбран статус *Закрыто*, необходимо выбрать решение.

   Если для инцидента была нарушена хотя бы одна метрика SLA, при закрытии инцидента отображается поле **Причины нарушения SLA**. В этом поле нужно указать причину нарушения SLA.

   > Если при изменении статуса *Закрыто* в рабочем процессе инцидента был установлен флажок **Разрешить закрывать только этот инцидент только пользователям с определенными разрешениями**, для закрытия инцидента необходима роль XDR Главный администратор или Подтверждающий.

   > Если вы измените статус инцидента на *Закрыт* и этот инцидент содержит незавершенные плейбуки или действия по реагированию, все связанные плейбуки и действия по реагированию будут прекращены.
5. Нажмите на кнопку **Сохранить**.

Статусы выбранных инцидентов будут изменены.

Статус инцидента также можно изменить с помощью плейбуков.

Изменение приоритета инцидента

Как объект, инцидент имеет приоритет, который определяет порядок, в котором инцидент должен расследоваться аналитиками. Вы можете изменить приоритет инцидента вручную.

> Если у вас есть право доступа на чтение и изменение алертов и инцидентов, вы можете изменять приоритеты инцидентов для своих инцидентов или инцидентов других аналитиков.

Инцидент может иметь один из следующих приоритетов:

- **Низкий**.
- **Средний** (значение по умолчанию).
- **Высокий**.
- **Критический**.

Инциденты с приоритетом **Критический** являются наиболее важными и должны быть расследованы в первую очередь. **Низкий** приоритет обычно означает, что инцидент помещен в очередь. Вы можете определить свои собственные критерии того, какой приоритет должен быть установлен для какого инцидента.

Чтобы изменить приоритет инцидента:

1. В главном окне приложения перейдите в раздел **Мониторинг → Инциденты**.
2. Выполните одно из следующих действий:
   - Установите флажки напротив инцидентов, которым требуется изменить приоритет.
   - Нажмите на идентификатор инцидента, чтобы открыть сведения об инциденте, приоритет которого вы хотите изменить.
3. Нажмите на кнопку **Изменить приоритет**.
4. В окне **Изменить приоритет** выберите приоритет, который нужно установить.
5. Нажмите на кнопку **Сохранить**.

   Приоритеты выбранных инцидентов будут изменены.

Также изменить приоритет инцидента можно с помощью плейбуков.

Для инцидента в статусе **Новый** (как только что созданного, так и переведенного в этот статус из любого другого):

- Вы можете редактировать приоритет, однако он автоматически пересчитывается при добавлении или удалении алерта из этого инцидента.

  Приоритет заполняется значением **Уровень важности инцидента**.
- Если вы вручную меняете приоритет инцидента, к которому не привязано ни одного алерта (инцидент создан без алертов либо все алерты удалены из инцидента), то **Уровень важности инцидента** заполняется значением приоритета.
- При пересчете приоритета SLA инцидента также пересчитывается автоматически.

Объединение инцидентов

Два или более инцидента могут быть интерпретированы как индикаторы одной и той же проблемы в ИТ-инфраструктуре организации. В этом случае вы можете объединить инциденты, чтобы исследовать их как единую проблему.

Когда вы объединяете инциденты, вам нужно выбрать среди них целевой инцидент. После объединения инцидента проблему необходимо исследовать в рамках целевого инцидента. Целевой инцидент должен иметь статус, отличный от статуса *Закрытый*. Остальные инциденты объединяются в целевой и после объединения получают статус *Закрытый* и решение **Объединено**.

Все алерты, связанные с объединенными инцидентами, автоматически связываются с целевым инцидентом. Так как у инцидента не может быть более 1000 связанных алертов, приложение считает алерты, связанные с инцидентами, которые вы хотите объединить. Если общее количество связанных алертов превышает 1000, выбранные инциденты не могут быть объединены. При выборе целевого инцидента, отображается общее количество алертов после слияния.

Вы не можете объединять дочерние инциденты или инциденты, у которых есть дочерние инциденты.

Чтобы объединить инциденты из таблицы инцидентов:

1. В главном окне приложения перейдите в раздел **Мониторинг → Инциденты**.
2. Установите флажки рядом с инцидентами, которые требуется объединить в целевой инцидент. На первом шаге мастера нужно будет выбрать целевой инцидент.
3. Нажмите на кнопку **Объединить в инциденте**.
4. Откроется мастер **Объединить инциденты**.
5. Выберите целевой инцидент.
6. Нажмите на кнопку **Объединить**.

   Инциденты объединены.

Чтобы объединить инциденты с использованием сведений об инциденте:

1. В главном окне приложения перейдите в раздел **Мониторинг → Инциденты**.
2. Нажмите на идентификатор инцидента, чтобы открыть сведения об инциденте. Этот инцидент будет объединен с целевым инцидентом. На первом шаге мастера нужно будет выбрать целевой инцидент.
3. Нажмите на кнопку **Объединить в инциденте**.

   Откроется мастер **Объединить инциденты**.
4. Выберите целевой инцидент.
5. Нажмите на кнопку **Объединить**.

   Инциденты объединены.

Экспорт инцидентов в файл

Вы можете экспортировать инциденты в файл PDF или JSON.

Чтобы экспортировать инцидент в файл PDF:

1. В главном окне приложения перейдите в раздел **Мониторинг → Инциденты**, чтобы открыть таблицу инцидентов.
2. Нажмите на идентификатор инцидента, который вы хотите экспортировать.
3. Нажмите на кнопку **Экспорт в PDF** в окне сведений инцидента.

   Откроется окно **Печать**.
4. В окне **Печать** разверните список **принтеров** и выберите **Сохранить как PDF**.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить инцидент в виде PDF-файла.

   Если отсортировать таблицу инцидентов по полям **Тип** или **Название**, экспортированный PDF-файл также будет использовать эту сортировку.

Чтобы экспортировать все инциденты в файл JSON:

1. В главном окне приложения перейдите в раздел **Мониторинг → Инциденты**, чтобы открыть таблицу инцидентов.
2. Нажмите на кнопку **Экспорт** в панели над таблицей событий.
3. Укажите имя файла и выберите папку, в которую нужно экспортировать инциденты.
4. Нажмите **Сохранить**, чтобы сохранить все инциденты в виде файла JSON.

Управление Service Level Agreement (SLA)

Kaspersky SIEM Cloud позволяет настраивать Service Level Agreement (SLA), которые определяют сроки обработки инцидентов.

Вы можете определить SLA для комбинации рабочего процесса инцидента и приоритета.

Таблица **Инциденты** и сведения об инцидентах показывают оставшееся время для SLA.

Вы можете настроить шаблон уведомления по электронной почте с типами **Истекает SLA инцидента** и **SLA инцидента изменено**.

Перезапуск расчета показателей SLA при возврате исходного статуса инцидента

Показатели SLA не рассчитываются для инцидента, когда инцидент считается обработанным. По умолчанию возврат статуса инцидента к исходному статусу приводит к перезапуску показателей SLA.

Чтобы предотвратить перезапуск показателей SLA при возврате исходного статуса инцидента:

1. Убедитесь, что на устройстве администратора установлена утилита kubectl.
2. Выполните следующую команду:

   ```
   kubectl -n irp set env deploy/incident
   OSMP_INCIDENT_SLA_DISABLE_RESTART_CALCULATION_ON_START_TRIGGER=true
   ```

3. Перезапустите службу инцидента.

Создание Service Level Agreement (SLA)

Для создания записей SLA у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, администратор SOC.

Чтобы создать SLA:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Откройте вкладку **Параметры** и нажмите **Управление инцидентами**.
4. Выберите вкладку **SLA** и нажмите на кнопку **Создать**.
5. В открывшейся панели **Создать SLA** настройте следующие параметры:

   - **Название SLA** – отображаемое имя SLA.
   - **Приоритет** – приоритет инцидента, к которому применяется SLA.
   - **Рабочий процесс** – рабочий процесс инцидента, к которому применяется SLA.

     Вы можете назначить только одно SLA для комбинации **Рабочий процесс** и **Приоритет**. Вы не можете выбрать рабочие процессы инцидентов, которые используются в других SLA с таким же приоритетом.

   - **Время на рассмотрение** – срок рассмотрения инцидента в днях, часах и минутах. Инцидент считается принятым, когда его статус меняется с одного на другой.

     Чтобы определить этот переход, выберите значения **Из статуса** и **В статус**.

   - **Время на ответ** – срок первоначального реагирования на инцидент в днях, часах и минутах.

     Выберите условие остановки:

     - Если вы хотите, чтобы инцидент считался обработанным после применения действия по реагированию, выберите **При первом действии по реагированию**. После этого выберите одно или несколько значений в поле **Из статуса**.
     - Если вы хотите, чтобы инцидент считался обработанным после того, как его статус изменился на другой, выберите **При смене статуса на**. После этого выберите одно или несколько значений в полях **Из статуса** и **В статус**.

- **Время на разрешение** – срок разрешения инцидента в днях, часах и минутах. Инцидент считается разрешенным, когда его статус меняется с одного на другой.

  Чтобы определить этот переход, выберите значения **Из статуса** и **В статус**.

6. Нажмите на кнопку **Создать**.

   Созданное SLA отобразится в таблице.

Удаление Service Level Agreement (SLA)

Для удаления записей SLA у вас должна быть одна из следующих XDR-ролей: Главный администратор, администратор тенанта, администратор SOC.

Чтобы удалить SLA:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

   Откроется список тенантов. Список содержит только те тенанты, к которым у вас есть хотя бы право на **Чтение**.

2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. Откройте вкладку **Параметры** и нажмите **Управление инцидентами**.

4. Выберите вкладку **Удалить**.

5. Установите флажок напротив SLA, которое нужно удалить.

6. Нажмите на кнопку **Удалить**.

7. В окне подтверждения нажмите на кнопку **Удалить**.

При удалении SLA сроки для инцидентов с указанием значений **Тип инцидента** и **Приоритет** больше не рассчитываются.

Работа с типами инцидентов

Kaspersky SIEM Cloud позволяет управлять инцидентами и настраивать процесс обработки инцидентов с помощью типов инцидентов.

Тип инцидента – это набор атрибутов, для которых вы можете настроить различные процессы, например, назначить рабочий процесс для типа инцидента, настроить триггер или алгоритм плейбука.

Вы можете создать тип инцидента или использовать предустановленные типы инцидентов, которые вы можете настроить.

Типы инцидентов могут быть активными или неактивными. Если тип инцидента активен, вы можете выбрать этот тип в окне с подробной информацией об инциденте.

Тип инцидента, отмеченный как тип по умолчанию, автоматически назначается всем новым инцидентам. Вы не можете переключить тип инцидента по умолчанию в неактивный.

Тип инцидента **Common** установлен как значение по умолчанию. Вы можете изменить этот параметр.

В тенанте вы можете создать только один тип инцидента по умолчанию.

Просмотр таблицы типов инцидентов

Чтобы просмотреть таблицу типов инцидентов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** нажмите на **Управление инцидентами**.

   Отобразится вкладка **Типы** с таблицей типов инцидентов.
4. Если вы хотите настроить таблицу типов инцидентов, выполните любое из следующих действий:
   - Нажмите на значок фильтрации ( ), укажите и примените критерий фильтрации в открывшемся меню.
   - Чтобы скрыть или отобразить столбец, нажмите на значок параметров ( ) и выберите нужный столбец.

В таблице типов инцидентов содержится следующая информация:

- **Название**. Название пользовательских или предустановленных типов инцидентов.

  В таблице содержатся следующие предустановленные типы инцидентов:
  - Общие.

    По умолчанию этот тип имеет значение **Да** в столбце **По умолчанию**.
  - Получение информации.
  - Компрометация.
  - Несанкционированный доступ.
  - Атака вредоносного ПО.
  - Фишинг.
  - Доступность.
  - Угроза изнутри.

    - Нарушение безопасности данных.
    - Ошибка конфигурации.
    - Атака через цепочку поставок.
    - Атака веб-приложения.
    - Использование уязвимостей.

- **Активный тип**. Если тип инцидента активен, вы можете выбрать этот тип в окне с подробной информацией об инциденте.
- **По умолчанию**. При создании инцидента, ему автоматически присваивается тип по умолчанию. Возможные значения:
    - **True.**
    - **False.**
- **Рабочий процесс**. Рабочий процесс инцидента.
- **Тенант**. Имя тенанта, которому принадлежит тип инцидента.
- **Тип создания**. Способ создания типа инцидента. Возможные значения:
    - **Пользовательский**
    - **Предопределенный**
- **Идентификатор**. Уникальный идентификатор пользовательского или предустановленного типа инцидента. По умолчанию этот столбец скрыт.
- **Описание**. Описание типа инцидента. По умолчанию этот столбец скрыт.

При необходимости, вы можете создавать новые типы инцидентов, а также изменять и удалять предустановленные и пользовательские типы инцидентов.

Создание типов инцидентов

Чтобы создать тип инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Типы**.
4. Нажмите на кнопку **Создать**.

   Откроется окно **Создать тип инцидента**.
5. Если вы хотите, чтобы новый тип инцидента был активным, включите переключатель **Активный тип**.

6. В поле **Название** введите название нового типа инцидента.
7. Если вы хотите, чтобы всем новым инцидентам по умолчанию назначался этот тип, установите флажок **Сделать по умолчанию**.

   В тенанте может быть только один тип инцидентов по умолчанию. Это означает, что, если у тенанта уже есть тип инцидента по умолчанию, этот тип больше не будет типом по умолчанию после того, как вы установите этот флажок.

8. В поле **Рабочий процесс** выберите рабочий процесс инцидента.
9. При необходимости в поле **Описание** укажите описание типа инцидента или комментарий.
10. Нажмите на кнопку **Создать**.

Новый тип инцидента отобразится в таблице типов инцидентов.

Изменение типов инцидентов

При необходимости вы можете изменять типы инцидентов.

Чтобы изменить тип инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.

3. На вкладке **Параметры** нажмите на **Управление инцидентами**.

   Отобразится вкладка **Типы** с таблицей типов инцидентов.

4. Нажмите на имя типа инцидента, который требуется изменить.

   Откроется окно **Изменить тип инцидента**.

5. Внесите изменения и нажмите на кнопку **Сохранить**. Дополнительные сведения о свойствах типов инцидентов, которые вы можете изменить, см. в разделе Создание типов инцидентов.

Свойства типа инцидента изменены и сохранены.

Управление типами рабочих процессов

Kaspersky SIEM Cloud позволяет настраивать гибкий рабочий процесс инцидента. Kaspersky SIEM Cloud также отображает рабочий процесс в визуальном редакторе.

Процесс обработки инцидента представляет собой набор статусов и переходов, через которые проходит инцидент в течение его жизненного цикла. *Статус* является шагом в процессе обработки инцидента. *Переход* помогает инциденту переходить в различные статусы. Переход – это ссылка, которая позволяет настраивать переходы от одного статуса инцидента к другому и обратно. При необходимости, вы можете использовать переход как однонаправленную ссылку.

Вы можете создать рабочий процесс инцидента или использовать предустановленный рабочий процесс, который можно настроить.

Также можно назначить рабочий процесс типам инцидентов. Это поможет вам управлять жизненным циклом инцидента наиболее удобным образом.

Просмотр таблицы рабочих процессов инцидентов

Чтобы просмотреть таблицу рабочих процессов инцидентов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Рабочие процессы**.

   Чтобы скрыть или отобразить столбец, нажмите на значок параметров (⚙) и выберите нужный столбец.

Отобразится таблица рабочих процессов инцидентов.

В таблице рабочих процессов инцидентов содержится следующая информация:

- **Название**. Название пользовательских или предустановленных рабочих процессов инцидентов.
- **Связанные типы**. Количество связанных типов инцидентов.
- **Имя тенанта**. Имя тенанта, которому принадлежит рабочий процесс инцидента.
- **Тип создания**. Способ создания рабочего процесса инцидента. Возможные значения:
  - **Пользовательский**.
  - **Предопределенный**.
- **Идентификатор рабочего процесса**. Уникальный идентификатор рабочего процесса инцидента. По умолчанию этот столбец скрыт.
- **Описание**. Описание рабочего процесса инцидента. По умолчанию, этот столбец скрыт.

Предустановленные рабочие процессы инцидентов

Kaspersky SIEM Cloud позволяет управлять инцидентами с помощью предустановленного рабочего процесса инцидента. В таблице рабочих процессов инцидентов, такой рабочий процесс называется **Стандартный**. В столбце **Тип создания** эти рабочие процессы отмечены как **Предопределенный**.

При необходимости, вы можете изменить предустановленный рабочий процесс.

В таблице ниже описаны статусы предустановленного рабочего процесса и причины, по которым инцидентам присваиваются эти статусы.

Состояние	Причины
Новый	• Инцидент создан (вручную или автоматически). • Статус инцидента был изменен на **Новый** с одного из следующих статусов: **В обработке**, **Отложен** или **Закрыт**.
В обработке	Пользователь вручную изменил статус инцидента с **Новый** или **Отложен** на **В обработке**.
Отложен	Пользователь вручную изменил статус инцидента с **В обработке** на **Отложен**.
Закрыт	• Пользователь закрыл инцидент. • Пользователь связал инцидент с другим похожим инцидентом, который еще не был закрыт.

Создание рабочих процессов инцидентов

Рабочий процесс инцидента позволяет управлять жизненным циклом инцидента.

Чтобы создать рабочий процесс инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Рабочие процессы**.
4. Нажмите на кнопку **Создать**.

   Откроется окно **Создать рабочий процесс**.

   > По умолчанию каждый рабочий процесс инцидента содержит предустановленные статусы **Новый** и **Закрыт**. Вы не можете удалить или изменить эти статусы.
5. В поле **Название** введите название нового рабочего процесса.
6. При необходимости в поле **Описание** введите описание рабочего процесса или комментарий.
7. Чтобы добавить новые статусы, в разделе **Рабочий процесс** нажмите **Добавить статус**.
8. В открывшемся окне настройте следующие параметры:

   a. В поле **Название статуса** введите название нового статуса.

   b. В поле **Категория** выберите одну из следующих категорий статуса:

   - **Новый**
   - **В обработке**
   - **Решен**
   - **Закрыт**

   Категория определяет цвет значка статуса.

c. В поле **Входящий переход** выберите один или несколько входящих статусов.

Если вы хотите настроить переход от всех статусов к входящим статусам, выберите параметр **Разрешить всем статусам переходить на этот**.

d. В поле **Исходящий переход**, выберите один или несколько исходящих статусов.

Если вы хотите настроить переход от исходящих статусов ко всем статусам, выберите параметр **Разрешить этому статусу переходить на все статусы**

e. Нажмите на кнопку **Добавить**.

Визуализированный рабочий процесс отображается в окне **Создать рабочий процесс**

При необходимости повторите шаги 7 и 8, чтобы добавить новые статусы.

9. В окне **Создать рабочий процесс** нажмите на кнопку **Сохранить**.

Новый рабочий процесс инцидента отобразится в таблице.

Изменение рабочих процессов и статусов инцидентов

Вы можете изменить свойства рабочего процесса, а также статусы и переходы рабочего процесса.

Чтобы изменить рабочий процесс инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Рабочие процессы**.
4. Выберите рабочий процесс, который требуется изменить.

   Откроется окно **Изменить рабочий процесс**.
5. Измените свойства рабочего процесса. Дополнительные сведения о свойствах рабочего процесса, которые вы можете изменить, см. в разделе Создание рабочего процесса инцидентов.

Свойства рабочего процесса изменены и сохранены.

Чтобы изменить статусы рабочего процесса инцидента:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры**, нажмите на **Управление инцидентами** и выберите вкладку **Рабочие процессы**.
4. Выберите рабочий процесс, который требуется изменить.

   Откроется окно **Изменить рабочий процесс**.
5. Нажмите на название статуса, который требуется изменить.

   Откроется окно **Изменить статус**.

6. Измените параметры статуса и параметры перехода. Дополнительные сведения о параметрах статуса, которые вы можете изменить, см. в разделе Создание рабочего процесса инцидентов.

   При необходимости, вы можете удалить статус, нажав на кнопку **Удалить**.

   > Вы не можете изменить название и категорию следующих предустановленных статусов: **Новый** и **Закрыт**. Вы также не можете удалить эти предустановленные статусы.

   > Вы не можете удалить статус, если он назначен инциденту.

7. Нажмите на кнопку **Сохранить**.

Статусы рабочего процесса изменены и сохранены.

Управление трудозатратами инцидентов

Kaspersky SIEM Cloud позволяет отслеживать трудозатраты на работу с инцидентами. Это помогает рассчитывать время, затрачиваемое аналитиком на анализ инцидентов и реагирование на них, оценивать рабочую нагрузку на аналитика и эффективным образом распределять трудовые ресурсы.

Аналитики могут вручную вводить данные о своих трудозатратах по работе с инцидентом, включая затраченное время и категорию трудозатрат, если это необходимо.

> Категории трудозатрат можно просматривать, добавлять, изменять или удалять через API. Чтобы управлять категориями трудозатрат, вам нужно иметь одну из следующих XDR-ролей: Главный администратор, Администратор тенанта, Администратор SOC.

> Для управления трудозатратами инцидентов у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Подтверждающий.

Kaspersky SIEM Cloud также позволяет формировать и экспортировать отчеты о трудозатратах аналитиков или групп пользователей для дальнейшего анализа.

Известные ограничения

В текущей версии решения названия категорий трудозатрат доступны только на русском языке. Перевод доступных категорий в следующей таблице:

ru-RU	en-US
Создание и оптимизация плейбуков	Playbooks creation and optimization
Мониторинг и обработка алертов	Alerts monitoring and processing
Расследование и реагирование на инциденты	Investigation and incident response
Отчетность и пост-анализ	Reporting and post-analysis

Проактивный поиск угроз	Threat Hunting
Обучение и поддержка команды	Training and team support

Добавление трудозатрат инцидентов

Вы можете добавить трудозатраты на работу с инцидентом в раздел **Журнал трудозатрат** подробных данных инцидента. Это помогает анализировать время, затрачиваемое аналитиками на обработку инцидентов, планировать свою рабочую нагрузку и рассчитывать затраты на заработную плату.

Чтобы добавить трудозатраты на работу с инцидентом:

1. В главном окне приложения перейдите в раздел **Мониторинг → Инциденты**.
2. В таблице инцидентов нажмите на идентификатор требуемого инцидента.

   Откроется окно со сведениями об инциденте.
3. Перейдите на вкладку **Журнал трудозатрат** и нажмите на кнопку **Добавить**.

   Откроется панель **Добавить трудозатраты**.
4. При необходимости в раскрывающемся списке **Категория** выберите категорию трудозатрат.
5. В полях **Часы** и **Минуты** укажите время, которое вы потратили на работу с инцидентом.

   > Максимальное значение поля **Минуты** – 59.
6. Нажмите на кнопку **Добавить**.

Трудозатраты на работу с инцидентами будут добавлены.

Изменения трудозатрат инцидентов

Вы можете изменить ранее добавленные трудозатраты.

> Невозможно изменять трудозатраты, добавленные другими аналитиками.

Чтобы изменить трудозатраты на работу с инцидентом:

1. В главном окне приложения перейдите в раздел **Мониторинг → Инциденты**.
2. В таблице инцидентов нажмите на идентификатор требуемого инцидента.

   Откроется окно со сведениями об инциденте.
3. Перейдите на вкладку **Журнал трудозатрат**.

4. В столбце **Дата** перейдите по ссылке с датой и временем трудозатрат, которые вы хотите изменить.

   Откроется панель **Изменить трудозатраты**.

5. Измените трудозатраты и нажмите на кнопку **Сохранить**.

Трудозатраты будут изменены и сохранены.

Удаление трудозатрат инцидентов

Вы можете удалить ранее добавленные трудозатраты.

Невозможно удалить трудозатраты, добавленные другими аналитиками.

Чтобы удалить трудозатраты на работу с инцидентом:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Инциденты**.
2. В таблице инцидентов нажмите на идентификатор требуемого инцидента.

   Откроется окно со сведениями об инциденте.

3. Перейдите на вкладку **Журнал трудозатрат**.
4. В списке трудозатрат установите флажки рядом с трудозатратами, которые вы хотите удалить и нажмите на кнопку **Удалить**.

Трудозатраты будут удалены.

Создание и экспорт отчетов об инцидентах

Вы можете формировать и экспортировать отчеты о трудозатратах аналитиков на работу с инцидентами и отчеты о соответствии инцидентов метрикам SLA. Отчеты сохраняются в формате CSV.

Чтобы сформировать отчет об инциденте, вам нужно:

- Иметь доступ к тенанту, к которому принадлежит инцидент.
- Иметь одну из следующих XDR-ролей: Главный администратор, Администратор SOC, Администратор тенанта, Младший аналитик, Аналитик 1-го уровня, Аналитик 2-го уровня, Менеджер SOC, Подтверждающий, Аудитор.

Чтобы сформировать и экспортировать отчет:

1. В главном окне приложения перейдите в раздел **Мониторинг → Инциденты**.
2. В панели инструментов нажмите на кнопку **Экспортировать** и в открывшемся меню выберите один из следующих вариантов:
   - **Отчет о трудозатратах** для экспорта трудозатрат аналитиков на работу с инцидентом.
   - **Отчет о метриках инцидента** для экспорта отчета о соответствии инцидентов показателям SLA.
3. В открывшейся панели укажите период, за который вы хотите отобразить данные в отчете. Для этого выберите дату и время в полях **От** и **По**.

   По умолчанию в поле **От** выбран первый день текущего месяца, а время установлено на 00:00. В поле **По** выбрана текущая дата и установлено время 23:59.
4. При необходимости укажите другие параметры в зависимости от типа отчета, который вы выбрали на шаге 3:
   - Если выбран **Отчет о трудозатратах**:
     - Выберите аналитиков или группы пользователей, чтобы в отчет были включены их трудозатраты на работу с инцидентами.
     - Включите переключатель **Включить идентификатор инцидента и сведения о категории трудозатрат**, если вы хотите, чтобы отчет о трудозатратах содержал эти сведения.

       По умолчанию переключатель выключен.
   - Если выбран **Отчет о метриках инцидента**:
     - Выберите приоритеты инцидентов, которые будут включены в отчет. Возможные значения: **Низкий**, **Средний**, **Высокий**, **Критический**.
     - Включите переключатель **Экспортировать только инциденты с нарушениями SLA**, если вы хотите включать в отчет только инциденты с нарушением SLA.

       Инцидент включается в отчет, если у него есть хотя бы одна запись SLA с истекшим сроком действия. Запись SLA истекла, если хотя бы одно из ее значений (**Время на рассмотрение**, **Время, использованное на ответ** или **Время на разрешение**) меньше 0.
5. Нажмите на кнопку **Экспортировать**.

Панель закроется, отчет будет создан и загружен на ваше устройство.

Настройка периода хранения алертов и инцидентов

Kaspersky SIEM Cloud позволяет вам уменьшать или увеличивать период хранения алертов и инцидентов в зависимости от ваших требований. По умолчанию период хранения алертов и инцидентов составляет 360 дней.

Чтобы настроить период хранения алертов или инцидентов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Нажмите на имя нужного тенанта.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** нажмите **Алерты и инциденты**.
4. В разделе **Срок хранения** укажите новый период хранения в одном или обоих полях:

   - **Срок хранения алерта (сут)**
   - **Срок хранения инцидента (сут)**

   Минимальное значение – `1`. Максимальное значение – `360`.
5. Нажмите на кнопку **Сохранить**.

Новый период хранения будет настроен.

Независимо от настроенного периода хранения, если истекший алерт связан с неистекшим инцидентом, алерт будет удален только после истечения периода хранения связанного инцидента. Если истекший инцидент имеет неистекшие связанные алерты, инцидент будет удален только после истечения периода хранения связанных алертов.

Просмотр информации об активе

Детали актива – это окно, которое содержит всю информацию, связанную с активом.

Вы можете просмотреть детали актива одним из следующих способов:

- из деталей алерта;
- из деталей инцидента;
- из деталей события (если событие содержит активы);
- Из графа расследования.

Чтобы просмотреть сведения об активе:

1. В главном окне приложения перейдите в раздел **Мониторинг** и выполните одно из следующих действий:

   - Если вы хотите просмотреть детали активов из деталей алерта, нажмите **Алерты**, а затем в столбце **Идентификатор** нажмите на идентификатор алерта, которое включает актив, детали которого вы хотите просмотреть. В открывшемся окне выберите вкладку **Активы**.
   - Если вы хотите просмотреть детали активов из деталей инцидента, нажмите **Инциденты**, а затем в столбце **Идентификатор** нажмите на идентификатор инцидента, который включает актив, детали которого вы хотите просмотреть. В открывшемся окне выберите вкладку **Активы**.

- Если вы хотите просмотреть детали активов из деталей события, нажмите **Поиск угроз**, а затем нажмите на событие, которое содержит актив, детали которого вы хотите просмотреть.

- Если вы хотите просмотреть детали активов из графа расследования, нажмите **Инциденты**, а затем в столбце **Идентификатор** нажмите на идентификатор инцидента, который включает актив, детали которого вы хотите просмотреть. В открывшемся окне нажмите на кнопку **Посмотреть на графе**. Нажмите на узел алерта и в контекстном меню выберите пункт **Устройства** или **Пользователи**.

2. Выполните одно из следующих действий:

   - Нажмите на имя требуемого актива и в раскрывающемся списке выберите **Просмотреть свойства**.

   - На графе расследования нажмите на узел актива, а затем в контекстном меню выберите пункт **Просмотреть информацию**.

   Отображается окно с деталями актива.

В окне информации об активе вы можете переключаться между вкладками **Общие** и **Правила запрета**.

Вкладка Общие

Вкладка **Общие** содержит следующие разделы:

- **Свойства актива** – информация об активе, например название актива, идентификатор и тенант, которому принадлежит актив.

- **Категории** – информация о категориях, связанных с активом.

- **Пользовательские поля** – поля активов, которые вы создали в веб-консоли.

- **Установленное программное обеспечение** – информация о программном обеспечении, установленном на активе.

  Вы можете использовать поле **Поиск**, чтобы быстро найти нужное приложение. Приложение отображается после того, как вы начинаете вводить любую информацию: название приложения, версию, производителя или дату установки.

- **KSC: уязвимости** – уязвимости актива, если есть. Эта информация доступна для активов, импортированных из Kaspersky Security Center.

- **Приложения "Лаборатории Касперского"** – информация о приложениях "Лаборатории Касперского", установленных на активе.

- **Состояние защиты устройства** – статус актива; возможны следующие значения: *OK*, *Критический*, *Предупреждение*. Эта информация доступна для активов, импортированных из Kaspersky Security Center.

- **KICS for Networks: свойства активов** – информация об активе. Эта информация импортируется из KICS for Networks.

- **KICS for Networks: уязвимости** – уязвимости актива, если есть. Эта информация доступна для активов, импортированных из KICS for Networks.

Вы можете расширить разделы, нажав на значки (>) рядом с их названиями.

В панели инструментов вы можете выполнить следующие действия:

- Изменить информацию об активе, нажав на кнопку **Изменить**.
- Запустить действие по реагированию, нажав на кнопку **Реагирование** и выбрав в раскрывающемся списке действие по реагированию.
- Назначить категорию активу, нажав на кнопку **Привязать к категории**.
- Перейти в раздел **История реагирований**, раздел **Поиск угроз**, в список связанных алертов или список связанных инцидентов.

  В разделах **История реагирований** и **Поиск угроз** алерты или инциденты будут отфильтрованы по активу, в сведения которого вы перешли.
- Экспортировать информацию об активах в CSV-файл, нажав на кнопку **Экспортировать в CSV**.

Вкладка правил запрета

Вкладка содержит таблицу правил запрета, примененных к устройству.

Правила запрета в таблице отображаются с одним из следующих статусов: **Применено, Применяется** или **Ошибка**.

> Для просмотра списка правил запрета у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Администратор SOC, Менеджер SOC, Аналитик 1-го уровня, Аналитик 2-го уровня, Младший аналитик, Подтверждающий, Аудитор.

В таблице те же столбцы, что и в таблице в разделе Ресурсы и сервисы.

Вы можете просматривать и изменять параметры правил запрета. Для этого откройте свойства правила запрета, перейдя по ссылке с названием правила в столбце **Имя**. Откроется панель **Изменить правило запрета** на вкладке **Подробнее**. Вы можете изменить параметры правила запрета.

Также вы можете нажать на кнопку **Перейти в Поиск угроз**, чтобы просмотреть события, полученные при срабатывании правила запрета. На вкладке **Журнал изменений** вы можете просмотреть все изменения правила запрета.

> Чтобы открыть сведения о правиле запрета, у вас должна быть одна из следующих XDR-ролей: Главный администратор, Администратор тенанта, Аналитик 1-го уровня, Аналитик 2-го уровня.
> Если правило запрета принадлежит родительскому тенанту, к которому у вас не доступа, вы не сможете изменить правило запрета.

Пример расследования инцидента с помощью Kaspersky SIEM

Выявление атаки на IT-инфраструктуру организации с помощью решения Kaspersky SIEM состоит из следующих шагов:

1. Предварительная подготовка
2. Назначение алерта пользователю
3. Проверка на соответствие между сработавшим правилом корреляции и данными событий алерта
4. Анализ информации об алерте
5. Проверка на ложное срабатывание
6. Определение критичности алерта
7. Создание инцидента
8. Расследование
9. Поиск связанных активов
10. Поиск связанных событий
11. Запись причин инцидента
12. Реагирование
13. Восстановление работоспособности активов
14. Закрытие инцидента

В описании шагов приводится пример действий по реагированию, которые мог бы выполнить аналитик при обнаружении инцидента в IT-инфраструктуре организации. Вы можете посмотреть описание и пример для каждого шага, перейдя по ссылке в его названии. Примеры относятся непосредственно к описываемому шагу.

Условия инцидента, для которого приводятся примеры, см. в разделе *Условия возникновения инцидента*.

Более подробную информацию о способах и инструментах реагирования вы можете посмотреть в документе *Руководство по реагированию на инциденты информационной безопасности*. На сайте Securelist "Лаборатории Касперского" вы также можете ознакомиться с дополнительными рекомендациями по выявлению инцидентов и реагированию.

Условия возникновения инцидента

Параметры компьютера (далее также "актива"), на котором произошел инцидент:

- ОС актива – Windows 10.
- Программное обеспечение актива – Kaspersky Endpoint Agent, Kaspersky Endpoint Security.

Параметры Kaspersky SIEM Cloud:

- Настроена интеграция с Active Directory, Open Single Management Platform, Kaspersky Endpoint Detection and Response.
- Установлены правила корреляции *SOC_package* из комплекта поставки решения.

Злоумышленник, заметив незаблокированный компьютер администратора, выполнил следующие действия на этом компьютере:

1. Скачал вредоносный файл со своего сервера.
2. Выполнил команду для создания ключа реестра в ветви `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`.
3. Добавил скачанный на первом шаге файл в автозапуск с помощью реестра.
4. Очистил журнал событий безопасности Windows.
5. Завершил сессию.

Шаг 1. Предварительная подготовка

Предварительная подготовка включает следующие этапы:

1. Мониторинг событий.

   Когда в Kaspersky SIEM Cloud создан и настроен коллектор, решение записывает события информационной безопасности, зарегистрированные на контролируемых элементах IT-инфраструктуры организации, в базу событий. Вы можете найти и просмотреть эти события.

2. Создание коррелятора и правил корреляции.

   При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции, решение создает алерты. Если для нескольких событий срабатывает одно и то же правило корреляции, все эти события привязываются к одному алерту. Вы можете использовать правила корреляции из комплекта поставки и создавать их вручную.

3. Настройка отправки уведомлений об алерте на один или несколько адресов электронной почты.

   Если отправка уведомлений настроена, при получении нового алерта Kaspersky SIEM Cloud отправляет на указанный адрес или адреса электронной почты уведомление. В уведомлении отображается ссылка на алерт.

4. Добавление активов.

   Вы можете выполнить на активе действия по реагированию (например, заблокировать запуск файла), только если актив добавлен в Kaspersky SIEM Cloud.

   > Для выполнения действий по реагированию необходима интеграция Kaspersky SIEM Cloud с Open Single Management Platform и Kaspersky Endpoint Detection and Response.

Пример

В рамках предварительной подготовки аналитик выполнил следующие действия:

- Установил и привязал к коррелятору правила корреляции *SOC_package* из комплекта поставки.
- Настроил отправку уведомлений об алертах на свой адрес электронной почты.
- Импортировал в Kaspersky SIEM Cloud активы из Open Single Management Platform.

Согласно условиям инцидента, после того, как администратор выполнил вход в свою учетную запись, был запущен вредоносный файл, который злоумышленник добавил в автозапуск Windows. От актива в Kaspersky SIEM Cloud поступили события из журнала событий безопасности Windows. Для этих событий сработали правила корреляции.

В результате в базу алертов Kaspersky SIEM Cloud были записаны следующие алерты:

- R223_Сбор информации о процессах.
- R050_Очистка журнала событий Windows.R295_Манипуляции с системой непривилегированным процессом.
- R097_Манипуляции с загрузочным скриптом.
- R093_Изменение критичных веток реестра.

В информации об алерте указаны названия правил корреляции, по которым были созданы алерты, и время первого и последнего событий, созданных при повторном срабатывании правил.

На адрес электронной почты аналитика пришли уведомления об алертах. Аналитик перешел по ссылке на алерт *R093_Изменение критичных веток реестра* из уведомления.

Шаг 2. Назначение алерта пользователю

Вы можете назначить алерт себе или другому пользователю.

Пример

В рамках рассматриваемого инцидента аналитик назначает алерт себе.

Шаг 3. Проверка на соответствие между сработавшим правилом корреляции и данными событий алерта

На этом этапе вам нужно просмотреть информацию об алерте и убедиться, что данные событий алерта соответствуют сработавшему правилу корреляции.

Пример

В названии алерта указано, что была изменена критичная ветвь реестра. В информации об алерте, в разделе **Показать связанные события** отображается таблица событий, относящихся к алерту. Аналитик видит, что в таблице записано одно событие, где указан путь к измененному ключу реестра, исходное и новое значение ключа. Следовательно, правило корреляции соответствует событию.

Шаг 4. Анализ информации об алерте

На этом этапе вам нужно проанализировать информацию об алерте, чтобы определить, какие данные требуется для дальнейшего анализа алерта.

Пример

Из информации об алерте аналитик узнает следующие данные:

- какой ключ реестра был изменен;
- на каком активе;
- имя учетной записи, под которой был изменен ключ.

Эту информацию можно просмотреть в информации о событии, вызвавшем создание алерта (**Алерты** → алерт *R093_Изменение критичных веток реестра* → **Показать связанные события** → событие 2022-08-23 17:27:05), в полях FileName, DeviceHostName, SourceUserName соответственно.

Шаг 5. Проверка на ложное срабатывание

На этом этапе вам нужно убедиться, что активность, по которой сработало правило корреляции, не является нормальной для IT-инфраструктуры организации.

Пример
На этом этапе аналитик проверяет, может ли обнаруженная активность быть легитимной в связи с нормальной работой системы (например, обновлением). В информации о событии видно, что под учетной записью пользователя с помощью утилиты *reg.exe* был создан ключ реестра. Также ключ реестра был создан в ветви `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, отвечающей за автозапуск программ при входе пользователя в систему. По этим данным можно определить, что активность не является легитимной и срабатывание не было ложным.

Шаг 6. Определение критичности алерта

При необходимости вы можете изменить уровень критичности алерта.

Пример
Аналитик присваивает алерту высокую степень критичности.

Шаг 7. Создание инцидента

Если в ходе выполнения шагов 3–6 становится понятно, что алерт требует расследования, вы можете создать инцидент.

Пример
Для проведения расследования аналитик создает инцидент.

Шаг 8. Расследование

Этот этап включает просмотр информации о связанных с инцидентом активах, учетных записях, алертах в информации об инциденте.

Информация о затронутых активах и учетных записях отображается на вкладке **Связанные активы** и **Связанные пользователи** в информации об инциденте.

Пример

Аналитик открывает информацию о затронутом в рамках инцидента активе (**Инциденты** → необходимый инцидент → **Связанные алерты** → необходимый алерт → **Связанные активы** → необходимый актив). В информации об активе видно, что актив привязан к категориям *Business impact/HIGH* и *Device type/Workstation*, которые являются критичными для IT-инфраструктуры организации.

Также в информации об активе могут быть полезны следующие данные:

- FQDN, IP-адрес и MAC-адрес актива.
- Время создания актива и последнего обновления информации.
- Количество алертов, с которыми этот актив связан.
- Категории, к которым привязан актив.
- Уязвимости актива.
- Информация об установленном программном обеспечении.
- Информация об аппаратных характеристиках актива.

Аналитик открывает информацию о связанной учетной записи пользователя (**Инциденты** → необходимый инцидент → **Связанные алерты** → ссылка с необходимым алертом → **Связанные пользователи** → учетная запись).

В информации об учетной записи могут быть полезны следующие данные:

- Имя пользователя.
- Имя учетной записи.
- Адрес электронной почты.
- Группы, в которых состоит учетная запись.
- Дата истечения пароля.
- Дата создания пароля.
- Время последнего неверного ввода пароля.

Шаг 9. Поиск связанных активов

Вы можете просмотреть алерты, которые происходили на связанных с инцидентом активах.

Пример

Аналитик проверяет другие алерты, которые происходили на связанных с инцидентом активах (**Инциденты** → необходимый инцидент → **Связанные алерты** → необходимый алерт → **Связанные активы** → необходимый актив → **Связанные алерты**). В окне с алертами можно настроить фильтрацию по времени или статусу, чтобы исключить устаревшие или уже обработанные алерты. По времени, в которое были записаны алерты актива, аналитик определяет, что эти алерты связаны между собой, поэтому их можно привязать к инциденту (отметить флажками необходимые алерты → **Привязать** → необходимый инцидент → **Привязать**).

Также аналитик находит связанные алерты для учетной записи и привязывает их к инциденту. Все связанные активы, которые были в новых алертах, также проверяются.

Шаг 10. Поиск связанных событий

Вы можете расширить расследование, выполнив поиск событий из связанных алертов.

События можно найти в базе событий Kaspersky SIEM Cloud вручную или выбрать любой из связанных алертов и в информации о нем нажать на кнопку **Найти в событиях** (**Инциденты** → необходимый инцидент → **Связанные алерты** → необходимый алерт → **Связанные активы** → **Найти в событиях**). Найденные события можно привязать к выбранному алерту, предварительно отвязав алерт от инцидента.

Пример

В результате поиска аналитику удалось найти событие *A new process has been created*, в котором была записана команда для создания нового ключа реестра. Исходя из данных события, аналитик обнаружил, что родительским процессом для `reg.exe` был `cmd.exe`. То есть злоумышленник запустил командную строку и выполнил команду в ней. В информации о событии была записана информация о файле *ChromeUpdate.bat*, для которого был выполнен автозапуск. Чтобы узнать происхождение этого файла, аналитик выполнил поиск событий по базе событий по полю `FileName = ‘C:\\Users\\UserName\\Downloads\\ChromeUpdate.bat’` и по маске доступа `%%4417` (тип доступа *WriteData (or AddFile)*):

```
SELECT * FROM 'events' WHERE DeviceCustomString1 like '%4417%' and FileName like
‘C:\\Users\\UserName\\Downloads\\ChromeUpdate.bat’ AND Device Vendor 'Microsoft' ORDER BY Timestamp DESC LIMIT 250
```

В результате поиска аналитик обнаружил, что файл был скачан из внешнего источника с помощью процесса `msedge.exe`. Это событие аналитик также привязал к алерту.

Произведя поиск связанных событий для каждого алерта инцидента, аналитик выявил всю цепочку атаки.

Шаг 11. Запись причин инцидента

Вы можете внести необходимую для расследования информацию в журнал изменений инцидента.

Пример
По результатам, полученным в ходе поиска связанных с инцидентом событий, аналитик выявил причины инцидента и записал результаты анализа в поле **Журнал изменений** в информации об инциденте, чтобы передать информацию другим аналитикам.

Шаг 12. Реагирование на инцидент

Вы можете выполнить следующие действия по реагированию:

1. Выполнить сетевую изоляцию актива.
2. Запустить антивирусную проверку.
3. Запретить запуск файла на активах.

Перечисленные действия доступны при интеграции Kaspersky SIEM Cloud с Open Single Management Platform и Kaspersky Endpoint Detection and Response.

Пример
У аналитика есть информация о связанных с инцидентом активах и об индикаторах компрометации, которая поможет в выборе действий по реагированию.

В рамках рассмотренного инцидента рекомендуется выполнить следующие действия:

- Запустить внеплановую антивирусную проверку актива, на котором был добавлен файл в автозапуск.
  Задача антивирусной проверки запускается через Open Single Management Platform.
- Изолировать актив от сети на время антивирусной проверки.
  Изоляция актива выполняется с помощью Kaspersky Endpoint Detection and Response.
- Поместить файл *ChromeUpdate.bat* в карантин и создать правила запрета на запуск этого файла на других активах организации.
  Правило запрета на запуск файла создается с помощью Kaspersky Endpoint Detection and Response.

Шаг 13. Восстановление работоспособности активов

После того как IT-инфраструктура будет очищена от следов присутствия злоумышленника, вы можете отключить правила запрета и сетевой изоляции активов в Kaspersky Endpoint Detection and Response.

Пример
После выполнения действий по расследованию, реагированию и очистке IT-инфраструктуры организации от следов атаки можно приступить к восстановлению работоспособности активов. Для этого можно отключить правила запрета на запуск файла и правила сетевой изоляции активов в Kaspersky Endpoint Detection and Response, если они не были отключены автоматически.

Шаг 14. Закрытие инцидента

После того как были приняты меры по очистке IT-инфраструктуры организации от следов присутствия злоумышленника, вы можете закрыть инцидент.

Поиск угроз

Страница **Поиск угроз** содержит инструменты, которые помогают анализировать события для поиска угроз и уязвимостей, которые не были обнаружены автоматически. Чтобы создать алерт из набора событий, выберите события и нажмите на кнопку **Создать алерт**.

Вы можете открыть страницу **Поиск угроз** любым из следующих способов:

- В главном окне приложения перейдите в раздел **Мониторинг → Поиск угроз**.
- В деталях алерта или инцидента в контекстном меню выберите пункт **Поиск в разделе Поиск угроз**.
- В сведениях об инциденте нажмите на кнопку **Посмотреть на графе**. В открывшемся графе расследования нажмите на кнопку **Поиск угроз**.

На странице **Поиск угроз** отображаются события. Вы можете отфильтровать события:

- изменив SQL-запрос;
- изменив период;
- выбрав тенант, которому принадлежат события.

Типовые сценарии поиска угроз

Работа с событиями

Раздел **Поиск угроз** содержит инструменты, которые помогут вам в поиске угроз и уязвимостей путем анализа событий.

Гранулярный доступ к событиям

В Kaspersky SIEM Cloud есть возможность обеспечить гранулярный доступ к событиям для пользователей с разными правами. Доступ к событиям регулируется на уровне пространств хранилища.

Вы можете назначить пользователям пространства в разделе **Доступ к пространствам** или прямо в карточке пользователя. Событие содержит идентификатор тенанта и пространства, поэтому пользователь должен обладать правами на соответствующий тенант и пространство, чтобы событие было доступно.

Следует учитывать следующие особенности отображения хранилищ:

- Если хранилища нет в разделе **Активные сервисы**, то хранилище и его пространства не отображаются в списке пространств набора.
- Если сервис хранилища был остановлен с помощью команды `systemctl stop kuma-<идентификатор хранилища>`, то хранилище и его пространства не отображаются в списке пространств набора.
- Если хранилище было запущено и далее удалено с помощью команды `uninstall`, то хранилище и его пространства продолжают отображаться в списке пространств набора.

В списке событий вы можете добавить в таблицу отображение поля **SpaceID**, в нем будет отображаться наименование пространства. Пространство событий аудита отображается как KUMA Audit. KUMA Default – пространство внутри каждого хранилища, куда передаются все события, если в хранилище отсутствуют настроенные пространства или если событие не попадает под условия наполнения существующих пространств.

При экспорте списка событий в файл TSV для пространств отображаются идентификатор и наименование пространства.

Чтобы разграничить доступ:

1. Назначьте пользователям соответствующие роли.
2. Настройте наборы пространств.

   Вы можете создать, изменить, удалить набор пространств. По результатам этих действий формируются события аудита.
3. Регулируйте права доступа к набору пространств: можно выдать или отозвать права доступа для выбранных пользователей.

Вы также можете посмотреть различные сценарии использования гранулярного доступа к событиям.

Просмотр таблицы событий

В таблице событий представлен обзор всех событий, полученных Ядром KUMA из источников данных. В таблице отображается список событий, отфильтрованных по выполненному SQL-запросу.

Чтобы просмотреть таблицу событий:

В главном окне приложения перейдите в раздел **Мониторинг → Поиск угроз**.

Отобразится таблица событий. Дополнительные сведения о столбцах таблицы см. в модели данных нормализованного события.

Поиск и фильтрация событий

При поиске событий создается событие аудита для запросов, выполняемых вручную.

События аудита не создаются для запросов, инициированных панелями мониторинга, отчетами или правилами сбора и анализа данных. Запросы REST API на получение событий также не генерируют событий аудита.

При использовании параметра GROUP BY в момент раскрытия группы создается событие аудита, поскольку для этого выполняется дополнительный запрос.

Если выбран вариант **Запуск в фоновом режиме**, создаются два события аудита: Event Read Attempt и Search Query Cancelled.

Для поиска и фильтрации событий измените SQL-запрос в поле поиска и нажмите на кнопку **Выполнить запрос**. Вы можете ввести SQL-запрос вручную или сгенерировать его с помощью конструктора запросов.

В SQL-запросах поддерживается агрегирование и группировка данных.

Вы можете добавить условия фильтрации к уже сформированному SQL-запросу в окне просмотра статистики, в таблице событий и в области сведений о событии.

Чтобы изменить параметры фильтрации из окна Статистика:

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Откройте область деталей **Статистика угроз** одним из следующих способов:
   - В правом верхнем углу таблицы событий нажмите на кнопку ••• и в выберите **Статистика угроз**.
   - В таблице событий нажмите на любое значение, а затем в открывшемся контекстном меню выберите пункт **Статистика угроз**.

   В правой части окна откроется область деталей **Статистика угроз**.
3. Откройте раскрывающийся список необходимого параметра и наведите курсор мыши на требуемое значение.
4. Измените параметры фильтрации, выполнив одно из следующих действий:
   - Чтобы включить только события с выбранным значением, нажмите на кнопку +.
   - Чтобы исключить все события с выбранным значением, нажмите на кнопку −.

Чтобы изменить параметры фильтрации в таблице событий:

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на значение параметра события в таблице событий.

3. В открывшемся меню выберите следующие параметры:

   - Чтобы оставить в таблице только события с выбранным значением, выберите **Искать события с этим значением**.
   - Чтобы исключить из таблицы все события с выбранным значением, выберите **Искать события без этого значения**.

Чтобы изменить параметры фильтрации в области сведений о событий:

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на соответствующее событие, чтобы открыть панель сведений о событии.
3. Измените параметры фильтрации, выполнив одно из следующих действий:

   - Чтобы включить только события с выбранным значением, нажмите на кнопку +.
   - Чтобы исключить все события с выбранным значением, нажмите на кнопку −.

В результате параметры фильтрации и таблица событий обновятся, а новый поисковый запрос отобразится в верхней части экрана.

> Когда вы переключаетесь на конструктор запросов, параметры запроса, введенного вручную в поле поиска, не передаются в конструктор, поэтому вам нужно будет создать запрос заново. Запрос, созданный в конструкторе, не перезаписывает запрос, введенный в строку поиска, пока вы не нажмете на кнопку **Применить** в окне конструктора.

Нажмите на кнопку , чтобы сохранить текущий фильтр.

Создание SQL-запросов вручную

С помощью строки поиска вы можете вручную создавать SQL-запросы любой сложности для фильтрации событий.

Выполнение SQL-запроса влияет на отображаемые столбцы таблицы.

Если SQL-запрос содержит значение *, указанные в запросе столбцы добавляются в таблицу, если они отсутствовали. Удаление отображаемого столбца из последующих запросов не скрывает соответствующий столбец.

Если SQL-запрос не содержит значения *, в таблице отображаются только столбцы для указанных полей, которые соответствуют нормализованной модели данных событий. Столбцы отображаются, даже если для них нет данных.

Чтобы сформировать SQL-запрос вручную:

1. Следуйте инструкциям, чтобы открыть таблицу событий.

2. Введите SQL-запрос в поле ввода.

   При вводе имени функции в поле SQL-запроса отображается список функций, которые можно использовать. При выборе функции справа отображается пример ее использования. Например, функция `concatWithSeparator` сопровождается следующим примером:

   ```
   concatWithSeparator('a', '1', '2', '3')
   ```

3. Нажмите на кнопку **Выполнить запрос**.

   Выполнение запроса может занять до нескольких минут.

   Вы также можете запустить выполнение запроса в фоном режиме. Для этого нажмите на значок стрелки рядом с кнопкой **Выполнить запрос** и выберите **Запустить в фоне**. В этом случае происходит следующее:

   - Запрос будет добавлен в очередь на выполнение в фоновом режиме, и в разделе **Обнаружение и реагирование** будет создана задача на выполнение этого запроса.
   - Фоновые запросы выполняются с низким приоритетом параллельно.
   - Запрос не может быть отправлен на выполнение в фоновом режиме, если он содержит более 10 000 событий.

   В таблице отобразятся результаты поиска по сформированному SQL-запросу. Результат выполнения запроса в фоновом режиме можно просмотреть в разделе **Обнаружение и реагирование**.

   При необходимости вы можете отменить выполнение запроса, нажав на значок стрелки рядом с кнопкой **Выполнить запрос** и выбрав **Отменить запрос**. При отмене запроса автоматически создается событие аудита.

   При необходимости вы можете отфильтровать события в таблице по периоду.

Чтобы отобразить непечатаемые символы в поле запроса SQL, нажмите любую из следующих комбинаций клавиш:

- **Ctrl+*/Command+***
- **Ctrl+Shift+8/Command+Shift+8**

Если вы включите отображение непечатаемых символов в компоненте XDR, другие компоненты (такие как KUMA) не будут автоматически отображать непечатаемые символы, пока вы не перезагрузите вкладки браузера компонентов.

Поддерживаемые функции и операторы

SELECT

Поля событий, которые следует возвращать.

Для **SELECT** в приложении поддержаны следующие функции и операторы:

Функции агрегации: **count**, **avg**, **max**, **min**, **sum**.

Арифметические операторы: **+**, **-**, *****, **/**, **<**, **>**, **=**, **!=**, **>=**, **<=**.

Вы можете комбинировать эти функции и операторы.

Если вы используете в запросе функции агрегации, настройка отображения таблицы событий, сортировка событий по возрастанию и убыванию, а также получение статистики недоступны.

FROM

Источник данных.

WHERE

Условия фильтрации событий.

- **AND**, **OR**, **NOT**, **=**, **!=**, **>**, **>=**, **<**, **<=**
- **IN**
- **BETWEEN**
- **LIKE**
- **ILIKE**
- **inSubnet**
- **match** (в запросах используется синтаксис регулярных выражений re2, специальные символы необходимо дополнительно экранировать с помощью обратной косой черты "\")

GROUP BY

Поля событий или псевдонимы, по которым следует группировать возвращаемые данные.

Если вы используете в запросе группировку данных, настройка отображения таблицы событий, сортировка событий по возрастанию и убыванию, получение статистики, а также ретроспективное сканирование недоступны.

ORDER BY

Столбцы, по которым следует сортировать возвращаемые данные.

Возможные значения:

- **DESC** – по убыванию.
- **ASC** – по возрастанию.

OFFSET

Пропуск указанного количества строк перед выводом результатов запроса.

LIMIT

Количество отображаемых в таблице строк.

По умолчанию указано значение 250.

При переключении на конструктор параметры запроса, введенного вручную в строке поиска, не переносятся в конструктор: вам требуется создать запрос заново. При этом запрос, созданный в конструкторе, не перезаписывает запрос, введенный в строку поиска, пока вы не нажмете на кнопку Применить в окне конструктора.

Используемые в поисковых запросах псевдонимы не должны содержать пробелов.

Примеры запросов:

- **SELECT * FROM `events` WHERE Type IN ('Base', 'Audit') ORDER BY Timestamp DESC LIMIT 250**

  Все события таблицы events с типом **Base** и **Audit**, отсортированные по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- **SELECT * FROM `events` WHERE BytesIn BETWEEN 1000 AND 2000 ORDER BY Timestamp ASC LIMIT 250**

  Все события таблицы events, для которых в поле **BytesIn** значение полученного трафика находится в диапазоне от 1000 до 2000 байт, отсортированные по столбцу **Timestamp** в порядке возрастания. Количество отображаемых в таблице строк – 250.

- **SELECT * FROM `events` WHERE Message LIKE '%ssh:%' ORDER BY Timestamp DESC LIMIT 250**

  Все события таблицы events, которые в поле **Message** содержат данные, соответствующие заданному шаблону %ssh:% в нижнем регистре, и отсортированы по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- **SELECT * FROM `events` WHERE inSubnet(DeviceAddress, '00.0.0.0/00') ORDER BY Timestamp DESC LIMIT 250**

  Все события таблицы events для устройств, которые входят в подсеть 00.0.0.0/00, отсортированные по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- **SELECT * FROM `events` WHERE match(Message, 'ssh.*') ORDER BY Timestamp DESC LIMIT 250**

  Все события таблицы events, которые в поле **Message** содержат текст, соответствующий шаблону ssh.*, и отсортированы по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- **SELECT max(BytesOut) / 1024 FROM `events`**

  Максимальный размер исходящего трафика (КБ) за выбранный период времени.

- **SELECT count(ID) AS "Count", SourcePort AS "Port" FROM `events` GROUP BY SourcePort ORDER BY Port ASC LIMIT 250**

  Количество событий и номер порта. События сгруппированы по номеру порта и отсортированы по столбцу **Port** в порядке возрастания. Количество отображаемых в таблице строк – 250.

  Столбцу **ID** в таблице событий присвоено имя Count, столбцу **SourcePort** присвоено имя Port.

- **SELECT * FROM `events` WHERE match(Message, 'ssh:\'connection.*') ORDER BY Timestamp DESC LIMIT 250**

  Если вы хотите указать в запросе специальный символ, вам требуется экранировать его, поместив перед ним обратную косую черту (\).

  Все события таблицы events, которые в поле **Message** содержат текст, соответствующий шаблону ssh: 'connection', и отсортированы по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

Формирование SQL-запроса с помощью конструктора

Вы можете сформировать SQL-запрос для фильтрации событий с помощью конструктора запросов.

Выполнение SQL-запроса влияет на отображаемые столбцы таблицы.

Если SQL-запрос содержит значение *, указанные в запросе столбцы добавляются в таблицу, если они отсутствовали. Удаление отображаемого столбца из последующих запросов не скрывает соответствующий столбец.

Если SQL-запрос не содержит значения *, в таблице отображаются только столбцы для указанных полей, которые соответствуют нормализованной модели данных событий. Столбцы отображаются, даже если для них нет данных.

Чтобы сформировать SQL-запрос с помощью конструктора:

1. Следуйте инструкциям, чтобы открыть таблицу событий.

2. Нажмите на кнопку , чтобы открыть конструктор запросов.

   Сформулируйте поисковый запрос, указав данные в следующих блоках параметров:

   - **SELECT**

     Поля событий, которые следует возвращать. По умолчанию выбрано значение *, означающее, что необходимо возвращать все доступные поля события. Чтобы настроить отображаемые поля, выберите нужные поля в раскрывающемся списке. Стоит учитывать, что Select * в запросе увеличивает длительность выполнения запроса, но избавляет от необходимости указывать поля в запросе.

     Выбрав поле события, вы можете в поле справа от раскрывающегося списка указать псевдоним для столбца выводимых данных, а в крайнем правом раскрывающемся списке можно выбрать операцию, которую следует произвести над данными: **count**, **max**, **min**, **avg**, **sum**.

   - **FROM**

     Источник данных. Выберите значение **events**.

   - **WHERE**

     Условия фильтрации событий.

     Чтобы добавить условия и группы, нажмите на кнопки **Добавить условие** и **Добавить группу**. Значение оператора **AND** выбирается по умолчанию в группе условий. Нажмите на значение оператора, чтобы изменить его. Доступные значения: **AND**, **OR**, **NOT**.

     Чтобы изменить структуру условий и групп условий, используйте значок ⠿ для перетаскивания выражений.

Чтобы добавить условия фильтрации:

a. В раскрывающемся списке слева выберите поле события, которое вы хотите использовать для фильтрации.

b. В среднем раскрывающемся списке выберите нужный оператор. Доступные операторы зависят от типа значения выбранного поля события.

c. Введите значение условия. В зависимости от выбранного типа поля может потребоваться ввести значение вручную, выбрав его из раскрывающегося списка или в календаре.

Чтобы удалить условия фильтрации, нажмите на кнопку **X**. Чтобы удалить условия группы, нажмите на кнопку **Удалить группу**.

- **GROUP BY**

  Поля событий или псевдонимы, по которым следует группировать возвращаемые данные.

  Если вы используете в запросе группировку данных, настройка отображения таблицы событий, сортировка событий по возрастанию и убыванию, получение статистики, а также ретроспективное сканирование недоступны.

- **ORDER BY**

  Столбцы, по которым следует сортировать возвращаемые данные. В раскрывающемся списке справа можно выбрать порядок: **DESC** – по убыванию, **ASC** – по возрастанию.

- **LIMIT**

  Количество отображаемых в таблице строк.

  По умолчанию указано значение 250.

  Если при фильтрации событий по периоду, указанному пользователем, количество строк в результатах поиска превышает заданное значение, вы можете отобразить в таблице дополнительные строки, нажав на кнопку **Показать больше записей**. Кнопка не отображается при фильтрации событий по стандартному периоду.

3. Нажмите на кнопку **Применить**.

   Текущий SQL-запрос будет перезаписан. Сгенерированный SQL-запрос отображается в поле поиска.

   Чтобы сбросить параметры конструктора, нажмите на кнопку **Запрос по умолчанию**.

   Чтобы закрыть конструктор, не перезаписывая существующий запрос, нажмите на кнопку .

4. Для отображения данных в таблице нажмите на кнопку **Выполнить запрос**.

   Выполнение запроса может занять до нескольких минут.

   Вы также можете запустить выполнение запроса в фоном режиме. Для этого нажмите на значок стрелки рядом с кнопкой **Выполнить запрос** и выберите **Запустить в фоне**. В этом случае происходит следующее:

   - Запрос будет добавлен в очередь на выполнение в фоновом режиме, и в разделе **Обнаружение и реагирование** будет создана задача на выполнение этого запроса.

   - Фоновые запросы выполняются с низким приоритетом параллельно.

   - Запрос не может быть отправлен на выполнение в фоновом режиме, если он содержит более 10 000 событий.

В таблице отображаются результаты поиска по сформированному SQL-запросу. Результат выполнения запроса в фоновом режиме можно просмотреть в разделе **Обнаружение и реагирование**.

При необходимости вы можете отменить выполнение запроса, нажав на значок стрелки рядом с кнопкой **Выполнить запрос** и выбрав **Отменить запрос**. При отмене запроса автоматически создается событие аудита.

При переходе в другой раздел веб-интерфейса сформированный в конструкторе запрос не сохраняется. Если вы повторно вернетесь в раздел События, в конструкторе будет отображаться запрос по умолчанию.

Формирование SQL-запроса с помощью SQL-функций Kaspersky SIEM Cloud

SQL-функции Kaspersky SIEM Cloud позволяют использовать атрибуты активов и учетных записей в поисковых запросах для фильтрации событий, формирования отчетов и виджетов (тип графика **Таблица**). Вы можете обогащать события, используя данные словарей, таблиц, активов и учетных записей с помощью следующих наборов функций:

- Набор функций enrich. Позволяет обогатить результаты запроса полями актива, учетной записи, значениями из словаря с типом **Словарь** и словаря с типом **Таблица**. Набор функций `enrich` включает в себя следующие функции:
  - `enrich_assets`;
  - `enrich_accounts`;
  - `enrich_table`;
  - `enrich_dictionary`.
- Набор функций lookup. Позволяет добавить в поисковый запрос условия по активам и учетным записям. Набор функций `lookup` включает в себя следующие функции:
  - `lookup_assets`;
  - `lookup_accounts`;
  - `lookup_assets_category`.

Максимальное количество событий в одном запросе – 10 000.

Использование набора функций enrich в SQL-запросах

Набор функций `enrich` (см. таблицу ниже) применяется в блоке `SELECT` SQL-запроса для обогащения результатов.

При использовании этого набора функций вы не можете группировать события по обогащенным полям.

Обогащаемые функциями виджеты и отчеты должны принадлежать не более чем одному тенанту.

Значения полей актива, которые указываются в SQL-запросах, являются регистрозависимыми.

Описание набора функций enrich

Функция	Поле события	Поле актива	Описание
enrich_assets	DeviceAssetID DestinationAssetID SourceAssetID	name os osBuild ipAddress macAddress fqdn source software cii ramSize kscLastAvBasesUpdate kscLastInfoUpdate kscLastUpdate kscLastSystemStart kscStatusMask kscRtProtectionState kscEncryptionState kscAntiSpamStatus kscEmailAvStatus kscDlpStatus kscStatusID kscEdrStatus lastVisible aistatus aiscore	Позволяет обогатить результат запроса полями актива на основании указанного в функции идентификатора. Пример enrich_assets(DeviceAssetID, name)

Функция	Поле события	Поле актива	Описание

`enrich_accounts`	`SourceAccountID`
	`DestinationAccountID`
		`name`
		`guid`
		`domain`
		`cn`
		`dn`
		`employee_id`
		`email`
		`mail_nickname`
		`mobile`
		`sid`
		`sam_name`
		`telephone_number`
		`principal_name`
		`sn`
		`type`
		`title`
		`division`
		`department`
		`manager`
		`location`
		`company`
		`street_address`
		`physical_delivery_office_name`
		`uac`
			Позволяет обогатить результат запроса полями учетной записи на основании указанного в функции идентификатора.
			
			Пример
			`enrich_account(SourceAccountID, name)`
			
			Функция доступна только для тенантов, у которых включено обогащение с помощью LDAP.

`enrich_table`	Любое	–	Позволяет обогатить результат запроса значениями из словаря с типом **Таблица** на основании полей событий в ответе от кластера ClickHouse.
			
			Пример
			`enrich_table('Main/some-table', [DeviceProduct], 'value')`
			
			Ключевой может быть только один столбец таблицы, но ключ записи может быть составным.
			
			Пример
			`enrich_table('Main/Dictionary', [BytesOut|BytesIn], 'value2')`
			
			Функция `enrich_table` возвращает только один столбец таблицы. Если надо вызвать больше столбцов, вызовите функцию повторно с указанием нужных полей.

`enrich_dictionary`	Любое	–	Позволяет обогатить результат запроса значениями из словаря с типом **Словарь** на основании полей событий в ответе от кластера ClickHouse.
			
			Пример 1
			`enrich_dictionary('Main/some-dict', [SourceAddress]`
			
			Пример 2
			`enrich_dictionary('Main/some-dict', [SourceAddress, DeviceAddress])`
			
			Вы можете посмотреть путь до словаря в разделе **Ресурсы** → **Словари**.

Вы можете задавать функцию `enrich` при ручном создании SQL-запросов.

Примеры запросов с функцией `enrich`:

Все события таблицы `events` с полями событий `Name` и `Message`, а также с полями актива `macAddress` и `osBuild` для обогащения результата данными актива. Количество отображаемых в таблице строк – 250.

```
SELECT Name,
Message,
   enrich_assets(DeviceAssetID, macAddress),
   enrich_assets(DeviceAssetID, osBuild)
FROM `events`
WHERE DeviceAssetID != ''
LIMIT 250
```

Все события таблицы `events` с полями событий `SourceUserName` и `SourceAddress`, а также со значениями поля `mobile` для обогащения результата данными учетной записи. Количество отображаемых в таблице строк – 10.

```
SELECT SourceUserName,
SourceAddress,
   enrich_accounts(SourceAccountID, mobile) as mobile
FROM `events`
WHERE SourceAccountID != ''
LIMIT 10
```

Все события таблицы `events` с полями событий `DeviceProduct` со значениями из таблицы **Main/[OOTB] Linux. Auditd record types**. Отсортированы по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 1000.

```
SELECT DeviceProduct,
   enrich_table('Main/[OOTB] Linux. Auditd record types', [DeviceProduct], 'Description') as HTTP
FROM `events` WHERE Type!=4
LIMIT 1000
```

Все события таблицы `events` с полями событий `DeviceAction` со значениями из словаря **Main/[OOTB] KEDR**. Количество отображаемых в таблице строк – 255.

```
SELECT DeviceAction,
   enrich_dictionary('Main/[OOTB] KEDR. AccountType', [BytesOut]) as accountType
FROM `events` WHERE Type!=4
LIMIT 255
```

Использование набора функций lookup в SQL-запросах

Набор функций `lookup` (см. таблицу ниже) применяется в блоке `WHERE` SQL-запроса для добавления в поисковый запрос условий по активам и учетным записям.

В запросы, содержащие функцию `lookup`, Kaspersky SIEM Cloud автоматически добавляет в выражение `SELECT` поле `*ID`, которое используется в функции `lookup` в запросе. Например, в запрос, содержащий функцию `lookup_assets(DeviceAssetID, osBuild, '=', '19045.000000')`, в выражение `SELECT` будет добавлено поле `DeviceAssetID`.

В запросах, содержащих функцию `lookup`, рекомендуется прописывать в функции `SELECT` список полей, которые необходимо возвращать. Не рекомендуется использовать в функции `SELECT` значение *. В этом случае будут возвращаться все доступные поля, что может значительно увеличить длительность выполнения запроса.

Тип функции	Поле события	Поле актива	Оператор	Описание

lookup_assets	DeviceAssetID
	SourceAssetID
	DestinationAssetID
		name
		os
		osBuild
		source
		cii
		ramSize
		kscRtProtectionState
		kscEncryptionState
		kscAntiSpamStatus
		kscEmailAvStatus
		kscDlpStatus
		kscStatusID
		kscEdrStatus
		aistatus
		aiscore
			=	Позволяет добавить в резул
				условия по активам, значени
				совпадают со значением, ука
				запросе.
				Для значений, которые являю
				надо указывать строку с нео
				числом.
				Например:
				`lookup_assets(DeviceAss`
				`'=', '19045.000000')`
				`lookup_assets(DeviceAss`
				`'=', '3241234234')`

		kscLastAvBasesUpdate
		kscLastInfoUpdate
		kscLastUpdate
		kscLastSystemStart
		lastVisible
		ramSize
		aiscore
			<
			>
			<=
			>=
				Позволяет добавить в резул
				условия по активам, значени
				• меньше значения, указан
				• больше значения, указан
				• меньше или равно значе
				в запросе;
				• больше или равно значе
				в запросе.
				Для значений, которые являю
				надо указывать строку с нео
				числом.
				Например:
				`lookup_assets(DeviceAss`
				`'>', '50')`
				Значения, которые являются
				указывать в следующих форм
				• Количество секунд:
				`lookup_assets(Device`
				`lastVisible, '>', '1`
				• Количество миллисекунд
				`lookup_assets(Device`
				`lastVisible, '<',`
				`'1725971837834')`
				• Количество дней:
				`lookup_assets(Device`
				`lastVisible, '<', 'n`

		name
		os
		osBuild
		fqdn
		software
			like	Позволяет добавить в резул
				условия по активам, значени
				соответствуют like-выражен
				запросе.
				Подробнее об операторе like
				Language Expressions.
				`lookup_assets(Destinati`
				`name, 'like','test.compa`

		ipAddress
		macAddress
		fqdn
		software
		kscStatusMask
			in	Позволяет добавить в резул
				условия по активам, значени
				соответствует значению, ука
				запросе.
				Например:
				`lookup_assets(DeviceAss`
				`'in', ['test_fqdn1.compa`
				`'test_fqdn2.company.ru'`

Тип функции	Поле события	Поле актива	Оператор	Описание

		`ipAddress`	`insubnet`	Позволяет добавить в резул
				условия по активам с IP-адре
				входят в указанную подсеть.
				указывается в формате CIDR
				Например:
				`lookup_assets(DeviceAss`
				`ipAddress, 'insubnet',`

		`ipAddress`	`inrange`	Позволяет добавить в резул
				условия по активам, IP-адрес
				попадает в указанный диапаз
				Первый указанный в запросе
				является начальным, второй
				Например:
				`lookup_assets(DeviceAss`
				`ipAddress, 'inrange', [`
				`'192.168.1.184'])`
				По результатам выполнения
				отфильтрованы активы с IP-а
				находящимися в диапазоне с
				192.168.1.184.

Тип функции	Поле события	Поле актива	Оператор	Описание

lookup_accounts	SourceAccountID
	DestinationAccountID
		name
		guid
		domain
		cn
		dn
		employee_id
		email
		mail_nickname
		mobile
		sid
		sam_name
		telephone_number
		principal_name
		sn
		title
		division
		department
		manager
		location
		company
		street_address
		physical_delivery_office_name
		uac
			=	Позволяет добавить в резул
				условия по учетным записям
				которых совпадают со значе
				в запросе.
				Для значений, которые являю
				надо указывать строку с нео
				числом.
				Например:
				`lookup_accounts(SourceA`
				`employee_id, '=', '1545`

		name
		guid
		domain
		cn
		dn
		employee_id
		email
		mail_nickname
		mobile
		sid
		sam_name
		telephone_number
		principal_name
		sn
		type
		title
		division
		department
		manager
		location
		company
		street_address
		physical_delivery_office_name
			like	Позволяет добавить в резул
				условия по учетным записям
				которых соответствуют like-в
				указанному в запросе.
				Подробнее об операторе like
				Language Expressions.
				`lookup_accounts(Destina`
				`name, 'like', '_ccount1`

Тип функции	Поле события	Поле актива	Оператор	Описание

`lookup_assets_category`	`DeviceAssetID`
	`SourceAssetID`
	`DestinationAssetID`
		–	–	Позволяет найти все событи связанные активы находятся папке.
				Например:
				`lookup_assets_category( ['Main/Business Impact']`
				где `Main` – это название тен `Impact` – название папки.

Примеры SQL-запросов с функцией lookup

Вы можете задавать функцию `lookup` при ручном создании SQL-запросов. Примеры запросов с функцией `lookup`:

- Все события таблицы events с полями событий `TenantID` и `DeviceProduct`, а также с полем актива `fqdn`, значение которого содержит подстроку `win10`. Количество отображаемых в таблице строк – 250.

```
SELECT TenantID, DeviceProduct
FROM `events`
WHERE DeviceAssetID != ''
AND lookup_assets(DeviceAssetID, fqdn, 'match', 'win10')
LIMIT 250
```

- Все события таблицы events с полями событий `TenantID` и `DeviceProduct`, а также со значениями поля `EmployeeID`, значение которого равно `15452`. Количество отображаемых в таблице строк – 10.

```
SELECT TenantID, DeviceProduct
FROM `events`
WHERE SourceAccountID != ''
AND lookup_accounts(SourceAccountID, employee_id, '=', '15452')
LIMIT 10
```

- Все события таблицы events с полями событий `TenantID` и `DeviceProduct`, а также с указанием папки, в которой находится актив. Количество отображаемых в таблице строк – 100.

```
SELECT TenantID, DeviceProduct
FROM `events`
WHERE DeviceAssetID != ''
AND lookup_assets_category(DeviceAssetID, ['Main/Business Impact'])
LIMIT 100
```

Просмотр сведений о событии

Чтобы открыть сведения о событии, выберите событие в таблице событий в разделе **Поиск угроз** или на странице деталей алерта.

Панель **Информация о событии** отображается в правой части окна веб-интерфейса и содержит список параметров события со значениями. В этой области вы можете:

- Включить выбранное поле в поиск или исключить его из поиска, нажав на + или на − рядом со значением параметра.
- Найти похожие события и добавить или удалить правило запрета, нажав на значения **FileHash** и **DeviceCustomString**.
- При интеграции с Kaspersky CyberTrace и Kaspersky Threat Intelligence Portal вы можете добавить в пользовательские сведения о киберугрозах CyberTrace и отобразить информацию из Поиска угроз (Threat Lookup), нажав на значения **FileHash** и **DeviceCustomString**.
- Просмотрите параметры службы, зарегистрировавшей событие, нажав на значение **Служба**.
- Просмотреть список алертов или инцидентов, связанных с устройством, нажав на значение **DeviceAssetID** и выбрав **Сведения об активе**. В открывшемся окне **Информация об устройстве** нажмите на кнопку **Показать связанные** и выберите **Алерты** или **Инциденты** в зависимости от того, что вы хотите просмотреть.

- Просмотр списка IOA-правил, сработавших при создании события; просмотр сведений об этих IOA-правилах, нажав на их названия.

  На открывшейся панели IOA-правило отображаются подробные сведения

  В открывшихся сведениях о правиле IOA доступны следующие действия:

  - Просмотр имени IOA-правила, идентификатора, уровня важности и уровня надежности.
  - Добавление IOA-правила в исключения.
  - Просмотреть информацию о поиске угроз, нажав на кнопку **Найти в Kaspersky TIP**.
  - По нажатию на кнопку **Открыть в** можно просмотреть алерты и инциденты, созданные при срабатывании правила IOA.
  - Просмотреть связанные события, нажав на кнопку **Найти в разделе "Поиск угроз"**.

    По умолчанию события отображаются за 24 часа.

  Вы также можете просмотреть подробную информацию о IOA-правиле в Kaspersky TIP. Для этого в окне сведений о IOA-правиле нажмите на кнопку **Найти в Kaspersky TIP**.

- Включите или выключите компактный режим отображения для `*Label`, нажмите на значок ⚙ и переведите переключатель в нужное положение. По умолчанию переключатель установлен в положение **Развернутый вид**. Если для полей `DeviceCustom*` и `Flex*` выбран режим **Компактный вид**, значение соответствующего поля `*Label` отображается как имя поля, а само поле `*Label` скрывается из списка полей событий. Если значение поля `*Label` отсутствует, отображается исходное название поля. Выбранный режим отображения сохраняется после обновления страницы и выхода из раздела **Поиск угроз**.

В панели **Информация о событии** вместо идентификатора отображается имя описываемого объекта в значениях следующих параметров. Если вы измените параметры фильтра в панели **Информация о событии**, в SQL-запрос будет добавлен идентификатор объекта, а не его имя:

- TenantID
- SeriviceID
- DeviceAssetID
- SourceAssetID
- DestinationAssetID
- SourceAccountID
- DestinationAccountID

Сохранение и выбор конфигурации фильтра событий

Вы можете сохранить текущую конфигурацию фильтра, включая временной фильтр, конструктор запросов и параметры таблицы событий, для использования в будущем. Сохраненные конфигурации фильтров доступны вам и другим пользователям, имеющим соответствующие права доступа.

Чтобы сохранить текущие параметры фильтра, запроса и периода

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на кнопку рядом с поисковым запросом и выберите пункт **Сохранить текущий фильтр**.
3. В открывшемся окне **Новый фильтр** введите название конфигурации фильтра в поле **Имя**. Имя должно содержать не более 128 символов Юникода.
4. В раскрывающемся списке **Тенант** выберите тенант, для которого нужно сохранить созданный фильтр.
5. Нажмите на кнопку **Сохранить**.

   Конфигурация фильтра сохранена.

Чтобы выбрать ранее сохраненную конфигурацию фильтра

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на кнопку рядом с поисковым запросом и выберите нужный фильтр.

Чтобы сохранить текущие параметры фильтра, запроса и параметры таблицы событий

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на значок шестеренки в панели над таблицей событий.
3. Нажмите на пункт **Сохранить текущий пресет**.
4. В открывшемся окне **Новый пресет** введите название пресета в поле **Имя**. Имя должно содержать не более 128 символов Юникода.
5. В раскрывающемся списке **Тенант** выберите тенант, для которого нужно сохранить созданный пресет.
6. Нажмите на кнопку **Сохранить**.

   Конфигурация пресета сохранена.

Чтобы выбрать ранее сохраненную конфигурацию пресета

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на значок шестеренки в панели над таблицей событий. Выберите вкладку **Пресеты**.
3. Выберите необходимый пресет.

Чтобы удалить ранее сохраненную конфигурацию фильтра для всех пользователей

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Нажмите на значок рядом с поисковым запросом.
3. Нажмите на значок рядом с конфигурацией, которую нужно удалить.
4. Нажмите на кнопку **OK**.

Фильтрация событий по периоду

Вы можете указать период для отображения событий.

Чтобы отфильтровать события по периоду:

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Откройте второй раскрывающийся список в верхней части окна.
3. Укажите период. Вы можете выбрать предопределенные периоды относительно текущей даты и времени или указать необходимый период, используя поля **Начало периода** и **Конец периода** или выбрав даты в календаре.
4. Нажмите на кнопку **Применить**.

Экспорт событий

Вы можете экспортировать информацию о событиях в файл TSV. Выборка событий, которые будут экспортированы в файл TSV, зависит от параметров фильтра. Информация экспортируется из столбцов, которые отображаются в таблице событий. Столбцы в экспортируемом файле заполняются доступными данными, даже если они не отображались в таблице событий в разделе **Поиск угроз** из-за особенностей SQL-запроса.

Чтобы экспортировать информацию о событиях:

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. В правом верхнем углу таблицы событий нажмите на кнопку ••• и в раскрывающемся списке выберите **Экспортировать в CSV**.

   Новая задача экспорта файла TSV создана в разделе KUMA **Диспетчер задач**.
3. В разделе KUMA, в подразделе **Диспетчер задач** найдите созданную вами задачу.
4. Нажмите на название типа задачи и выберите в раскрывающемся списке пункт **Загрузить**.

   Файл TSV будет загружен с использованием параметров вашего браузера. По умолчанию имя файла event-export-<date>_<time>.tsv.

Файл сохранен в соответствии с параметрами вашего браузера.

Экспорт событий в хранилище S3

Kaspersky SIEM Cloud позволяет экспортировать найденные события из облачного хранилища телеметрии в собственное совместимое хранилище S3. При экспорте Kaspersky SIEM Cloud формирует файл в формате TSV и сохраняет его по пути, указанному для хранилища S3.

Перед экспортом событий нужно настроить хранилище S3.

Экспорт событий в хранилище S3 доступен пользователям со следующими ролями: Аналитик 1-го уровня, Аналитик 2-го уровня, Младший аналитик, Администратор тенанта и Главный Администратор.

Чтобы экспортировать события в хранилище S3:

1. В веб-консоли перейдите в раздел **Мониторинг** → **Поиск угроз** или откройте список событий из карточки алерта.

2. При необходимости настройте поисковый запрос, условия фильтрации, набор и порядок столбцов в таблице событий.

   При экспорте учитываются условия фильтрации, заданные для поиска событий.

   Если в поисковом запросе используется выборка отдельных полей с помощью оператора `SELECT`, в экспортируемый файл все равно попадают все поля событий. Например, если используется запрос `SELECT BytesIn, BytesOut FROM events LIMIT 250`, в таблице событий будут заполнены выбранные поля `BytesIn` и `BytesOut`, а также поля, которые отображаются независимо от выборки (`Timestamp` и `Type`). Остальные поля таблицы могут оставаться пустыми. При экспорте результатов поиска в файл будут включены все поля событий, а не только `BytesIn` и `BytesOut`.

3. В таблице со списком событий нажмите на кнопку **Экспортировать в S3** и выберите один из следующих вариантов:

   - **Выбранные столбцы** – экспортировать только выбранные столбцы.

     Используйте этот вариант, если нужно экспортировать только столбцы, выбранные для отображения в таблице событий, включая столбцы с пустыми значениями. При экспорте также сохраняется порядок столбцов, установленный в таблице событий.

   - **Все столбцы** – экспортировать все столбцы.

     Используйте этот вариант, если нужно экспортировать все доступные поля событий независимо от того, какие столбцы выбраны для отображения в таблице, включая поля с пустыми значениями. Поля располагаются в алфавитном порядке, при этом порядок столбцов, установленный в таблице событий, не сохраняется.

   Kaspersky SIEM Cloud сформирует файл в формате TSV. В качестве разделителя между полями используется символ табуляции (`\t`).

   Имя файла формируется автоматически по следующему шаблону:

   ```
   event-export-<YYYY-MM-DD>_<HHMMSS>
   ```

где:

- `<YYYY-MM-DD>` – дата создания файла;
- `<HHMMSS>` – время создания файла.

Пример

```
event-export-2026-11-08_135920.tsv
```

Экспортируемые файлы будут сохранены в хранилище S3 по пути, который вы указали при настройке хранилища в Kaspersky SIEM Cloud.

Просмотр событий аудита и настройка уведомлений

Аудит – это процесс мониторинга, регистрации и анализа действий пользователей и системных операций, направленных на обеспечение безопасности и контроль изменений.

Kaspersky SIEM Cloud получает события аудита от компонентов решения автоматически, дополнительная настройка не требуется. Во время развертывания решения Kaspersky SIEM Cloud создает предустановленный коллектор **[OOTB] Kaspersky OSMP** в корневом тенанте. У этого коллектора есть предустановленный коннектор **[OOTB] Kaspersky OSMP** и предустановленный нормализатор **[OOTB] Kaspersky OSMP audit**. Коллектор отправляет события аудита в пространство хранилища **KUMA Audit**. Это пространство хранилище создается автоматически.

Kaspersky SIEM Cloud получает события аудита только в том случае, если вы указали действительный лицензионный ключ для SIEM-компонента в параметре `license` во время развертывания на одном узле, развертывания на нескольких узлах или в интерфейсе решения.

При необходимости вы можете настроить параметры хранилища для событий аудита, если создаете набор ресурсов для хранилища.

Подробная информация о параметрах и типах действий аудита приведена в статье События аудита.

Как просмотреть и экспортировать события аудита в файл

События аудита доступны в разделе **Мониторинг → Поиск угроз**.

Если вы хотите, чтобы в таблице событий отображались только события аудита, выполните одно из следующих действий:

- В таблице событий в поле **EventType** установите значение `Audit`.
- Разграничьте доступ к пространству с помощью событий аудита.

  Для этого перейдите в раздел **Параметры → KUMA → Открыть параметры KUMA → Доступ к пространствам** и настройте права доступа к пространству KUMA Audit. Только пользователи, которым предоставлены права доступа к пространству, смогут просматривать события аудита в разделе **Поиск угроз**.

После фильтрации событий аудита в таблице вы можете экспортировать события в файл.

Как настроить уведомление по электронной почте о событиях аудита

Как только происходит событие, например, пользователь выполняет более пяти неудачных попыток входа в Консоль OSMP, срабатывает предопределенное правило корреляции и создается алерт.

Если вы хотите получать уведомления об алертах по электронной почте, вам нужно создать шаблон уведомления. В панели **Создать шаблон электронной почты** укажите следующие параметры:

- В раскрывающемся списке **Тип события** выберите тип шаблона уведомления **Создание алерта**.
- В раскрывающемся списке **Правила корреляции** выберите предустановленное правило корреляции.

Ретроспективное сканирование

Вы можете использовать ретроспективное сканирование (retroscan), чтобы уточнить ресурсы правил корреляции или проанализировать данные истории.

Вы также можете создавать алерты на основе функции ретроспективного сканирования (retroscan).

Чтобы использовать ретроспективное сканирование:

1. В главном окне приложения перейдите в раздел **Мониторинг** → **Поиск угроз**.
2. В правом верхнем углу таблицы событий нажмите на кнопку ••• и в выберите **Ретроспективное сканирование**.

   Откроется панель **Ретроспективное сканирование**.
3. В раскрывающемся списке **Коррелятор** выберите пункт Коррелятор, в который будут передаваться выбранные события.
4. В раскрывающемся списке **Правила корреляции** выберите правила корреляции, которые необходимо использовать при обработке событий.
5. Чтобы выполнить действия по реагированию во время обработки событий, включите переключатель **Выполнить действия по реагированию**.
6. Чтобы генерировать алерты во время обработки событий, включите переключатель **Создать алерты**.
7. Нажмите на кнопку **Создать задачу**.

   Задача ретроспективного сканирования создана в разделе KUMA **Диспетчер задач**.

Получение статистики таблицы событий

Вы можете получить статистику по выбранным событиям, отображаемым в таблице событий. Выбранные события зависят от параметров фильтра.

Чтобы получить статистику:

1. Следуйте инструкциям, чтобы открыть таблицу событий.
2. Выполните одно из следующих действий:
   - В верхнем правом углу таблицы событий выберите **Статистика** из раскрывающегося списка •••.
   - В таблице событий нажмите на любое значение и в контекстном меню выберите пункт **Статистика**.

Отобразится область сведений раздела **Статистика** со списком параметров из текущей выборки событий. Цифры возле каждого параметра означают количество событий с этим параметром в выборке. Если параметр развернут, отображаются пять наиболее часто встречающихся значений. Введите название параметра в **Поля поиска** для фильтрации отображаемых данных.

Окно **Статистика** позволяет изменять фильтр событий.

При использовании SQL-запросов с группировкой и агрегированием данных для фильтрации событий статистика недоступна.

AI-сервисы

В этом разделе представлена информация об AI-сервисах, с которыми работает Kaspersky SIEM Cloud.

Использование AI-ассистента KIRA

Вы можете использовать Kaspersky Investigation and Response Assistant (далее также KIRA) для анализа алертов и инцидентов. По итогам анализа вы получаете автоматически созданное описание алерта или инцидента, которое включает в себя краткую сводку, список наблюдаемых объектов, временную шкалу событий, отчет по алерту или инциденту и рекомендации по устранению уязвимостей.

Эта функция может ускорить расследование и первоначальный анализ алертов или инцидентов безопасности. Она доступна вне зависимости от того, какие типы событий связаны с алертом или инцидентом.

При использовании стороннего LLM-провайдера, запрос отправляется непосредственно в указанный API. Выбор провайдера и модели, а также настройку параметров выполняет пользователь. Обработка данных осуществляется на стороне выбранного сервиса.

Kaspersky SIEM Cloud поддерживает работу со следующими сторонними LLM-провайдерами:

- GPT-5.4
- Deepseek-V4-Pro
- Kimi K2.6

- GLM-5.1
- MiniMax M2.7

Функция доступна при выполнении следующих условий:

- Наличие действующей лицензии с модулем AI.

  Если срок лицензии истек, результаты анализа будут доступны через задачи в течение 14 дней с момента попадания результатов в кеш.

- Настроено подключение к API стороннего LLM-провайдера.
- Пользователю назначена одна из ролей с правами доступа: Главный администратор, Администратор, Аналитик 2-го уровня, Аналитик 1-го уровня, Младший аналитик.

  Настройка интеграции доступна только пользователю с ролью Главный администратор.

Настройка интеграции с KIRA с использованием LLM-провайдера

Для наглядного ознакомления с настройкой интеграции с использованием LLM-провайдера вы можете просмотреть видео ниже.

Чтобы настроить интеграцию с KIRA с использованием стороннего LLM-провайдера:

1. Получите лицензию с AI-модулем и активируйте функциональность в Kaspersky SIEM Cloud.
2. В веб-консоли откройте раздел **Параметры** → **KUMA** → **Открыть параметры KUMA**.
3. В разделе **Интеграции** нажмите **AI-сервисы**.
4. В открывшемся окне перейдите на вкладку **Kaspersky Investigation & Response Assistant**.
5. Включите интеграцию с KIRA, установив переключатель **Состояние** в активное положение.

   По умолчанию переключатель выключен.
6. В поле **Базовый URL-адрес** укажите API-адрес провайдера (например: `https://api.openai.com/v1`). Адрес должен начинаться с `http://` или `https://`.
7. В раскрывающемся списке **API ключ** выберите секрет типа **token** или создайте новый.

Как создать секрет

Чтобы создать секрет:

1. В поле **Имя** введите название секрета.
2. В поле **Токен** введите токен.
3. При необходимости в поле **Теги** укажите теги для секрета.
4. При необходимости в поле **Описание** введите описание секрета.
5. Нажмите на кнопку **Создать**.

   Секрет будет добавлен и отобразится в раскрывающемся списке **Секрет**.

Если используемый API не требует ключа, в поле **API ключ** укажите секрет со значением **api-key**.

8. В поле **Модель** укажите имя модели, используемой провайдером (например: `gpt-4-turbo`, `llama3-70b`).
9. В поле **Максимальный размер промпта** укажите максимальное количество токенов в запросе.
10. Нажмите на кнопку **Загрузить файл JSON**, чтобы загрузить файл с заданными параметрами модели и HTTP-заголовками.

    Вы можете указать в файле дополнительные параметры запроса к LLM-провайдеру (например `temperature`, `max_tokens`). Также вы можете задать дополнительные HTTP-заголовки. Для этого нужно использовать ключ `"headers"`. Если в файле указано несколько ключей `"headers"`, используется только первый из них.

    Пример содержания файла

    ```
    {
      "temperature": 0.5,
      "max_tokens": 20000,
      "headers": {
        "OpenAI-Organization": "ORG_ID"
      }
    }
    ```

    Если в JSON-файле указан хотя бы один из следующих параметров, AI-сервис вернет ошибку: `messages`, `model`, `audio`, `function_call`, `functions`, `modalities`, `n`, `parallel_tool_calls`, `prediction`, `response_format`, `stop`, `stream`, `stream_options`, `tool_choice`, `tools`, `web_search_options`.
11. Нажмите **Проверить подключение**, чтобы выполнить тестовый запрос к указанному API.
12. Нажмите **Сохранить**.

    После того как вы нажмете **Сохранить**, вам будет предложено принять условия Лицензионного соглашения. Если вы не примете соглашение, сохранить параметры и продолжить работу с KIRA будет невозможно.

    После сохранения параметров будет показано доступное количество токенов. Количество токенов обновляется ежедневно.

Интеграция будет настроена, можно переходить к анализу. Анализ доступен для всех событий, новых и уже полученных.

Выполнение анализа с помощью KIRA

После того как интеграция настроена, можно выполнять анализ алертов и инцидентов с помощью KIRA.

Чтобы выполнить анализ:

1. Откройте детали алерта или инцидента.
2. На панели инструментов в верхней части раздела деталей алерта или инцидента нажмите **AI-анализ** → **Проанализировать с помощью KIRA**.

   Если достаточно токенов, запустится выполнение анализа и задача **Запрос в KIRA**.

   Выполнение запроса может занимать от 30 секунд и дольше.

   Расход токенов осуществляется, даже если получен ответ с ошибкой о том, что запрашиваемая тема находится в запрещенном списке, при этом сведения о доступном остатке токенов тоже будут обновлены.

Анализ алерта или инцидента будет выполнен.

Чтобы просмотреть результаты анализа, на панели инструментов в верхней части раздела деталей алерта или инцидента нажмите **AI-анализ** → **Просмотр отчета**. В окне **Проанализировать с помощью KIRA** отображается результат анализа, который включает в себя следующую информацию:

- краткое описание алерта или инцидента;
- список наблюдаемых объектов;
- хронологию событий, связанных с алертом или инцидентом, с временной шкалой;
- отчет о происшествии;
- дату и время последнего запроса;
- количество израсходованных токенов.

Вы можете нажать на кнопку **Повторный анализ**, чтобы выполнить новый анализ без учета данных предыдущего, хранящихся в кеше. При проведении этого анализа будут израсходованы токены.

Возможные ошибки задачи Проанализировать с помощью KIRA

При проведении анализа алертов и инцидентов с помощью KIRA могут возникать ошибки.

Возможные ошибки

HTTP-код	Описание
400	Неверный запрос к службе или недействительный клиентский сертификат. Возможные причины: необходимые параметры отсутствуют или содержат недопустимые значения; срок действия клиентского сертификата, используемый для KSN, истек, или сертификат выдан ненадежным центром сертификации.
401	Не удалось выполнить аутентификацию. Клиентский сертификат действителен, но в базе данных лимитов нет соответствующей ему записи. Возможные причины: запись была удалена или не была своевременно создана, либо из-за технической ошибки были записаны неверные данные.

HTTP-код	Описание
403	Ежедневное ограничение по токенам превышено.
404	Неизвестная или не поддерживаемая пользовательская задача
413	Превышен лимит токенов для запроса. Запрос содержит слишком много входных токенов. Максимально допустимое количество токенов на один запрос – 16 000, включая параметры службы. Если этот предел превышен, анализ не будет проведен.
500	Внутренняя ошибка службы. При обработке запроса произошла неизвестная ошибка.
502	AI-сервис недоступен. KIRA недоступен.
503	Ошибка подключения службы. Не удалось получить токен доступа от KIRA.
Другое	Ошибка подключения. Любой другой код ошибки, не указанный выше, который возвращает службу KSN.
Без кода	Ошибка при обработке запроса на стороне Kaspersky SIEM Cloud. Возможные причины включают ошибку при чтении ответа от KSN, ошибку при сохранении данных в базе данных или ошибку при получении параметров интеграции.

Генерация регулярных выражений с помощью KIRA

Вы можете автоматически создать одно или несколько регулярных выражений на основе примеров событий для нормализатора с методом парсинга **regexp** с помощью Kaspersky Investigation and Response Assistant. Эта функция доступна пользователям с ролями Главный администратор, Администратор тенанта, Аналитик второго уровня, Аналитик первого уровня, Младший аналитик.

Чтобы сгенерировать регулярные выражения:

1. Получите лицензию с AI-модулем и активируйте функциональность в Kaspersky SIEM Cloud.
2. Настройте интеграцию с KIRA с использованием стороннего LLM-провайдера (режим **Custom**).
3. Запустите создание нормализатора или откройте параметры существующего нормализатора.
4. На вкладке **Схема нормализации** в раскрывающемся списке **Метод парсинга** выберите **regexp**.
5. В поле **Примеры событий** добавьте один или несколько примеров событий, на основе которых требуется создать регулярное выражение.

   Вы можете добавить не более 10 однострочных событий.
6. Нажмите на кнопку **Сгенерировать регулярное выражение с помощью KIRA**.
7. Подтвердите отправку запроса.

   После обработки запроса откроется окно, в котором отображаются:

   - количество оставшихся токенов (если у вас настроена интеграция с KIRA с использованием KSN);
   - количество токенов, использованных при генерации;
   - сгенерированные регулярные выражения с цветовой подсветкой групп и соответствующих фрагментов примеров событий.

   Каждое сгенерированное регулярное выражение содержит в начале группу символов (?:ai)?.

   В окне с созданными выражениями вы можете отредактировать и скопировать регулярное выражение, а также применить результат генерации, нажав на кнопку **Применить**.

Если генерация регулярного выражения завершается ошибкой или не дает ожидаемого результата, это может означать, что используемая модель провайдера не смогла правильно определить компоненты события или сформировать регулярное выражение. Попробуйте запустить генерацию повторно. Если ошибка повторяется, добавьте в поле **Примеры событий** несколько других похожих примеров и запустите генерацию повторно. При запуске генерации после ошибки дополнительные токены не используются.

После применения результата сгенерированное регулярное выражение автоматически добавляется в поле **Нормализация**. Если было сгенерировано несколько регулярных выражений, автоматически создается соответствующее количество полей для каждого выражения. Регулярные выражения добавляются в порядке их генерации, который при необходимости можно изменить, перетаскивая выражения с помощью значка ⠿.

8. После применения результата генерации регулярных выражений сохраните параметры нормализатора, нажав на кнопку **OK** и затем на кнопку **Сохранить**.

Обнаружение атак DLL Hijacking

DLL Hijacking – это техника атаки, которая заключается в том, что на целевую систему вместе с уязвимым легальным программным обеспечением доставляется вредоносная динамическая библиотека (DLL). Уязвимое программное обеспечение при запуске не проверяет легитимность динамической библиотеки и загружает ее по имени файла, в результате чего запускается вредоносный код. Атаку с использованием техники DLL Hijacking сложно обнаружить, так как фактически запускается легальное программное обеспечение.

Для обнаружения атак типа DLL Hijacking используется модуль AI, который анализирует параметры запуска и исполнения программ и определяет подозрительные случаи запуска легального программного обеспечения с вредоносными библиотеками. Для того чтобы настроить модуль AI, при создании правила обогащения нужно выбрать тип **Проверка DLL Hijacking** и затем привязать его либо к коллектору, либо к коррелятору. Мы рекомендуем привязывать обогащение этого типа к коррелятору, а не к коллектору, поскольку в корреляторе проверка проводится на корреляционном событии, а в коллекторе – на базовом. Так как корреляционных событий намного меньше, чем базовых, запросов для проверки корреляционных событий требуется намного меньше. Таким образом, при проверке в корреляторе нагрузка на службу KSN значительно ниже, чем при проверке событий в коллекторе.

Для получения заключения Kaspersky SIEM Cloud отправляет запрос в KSN. Запрос содержит информацию из полей события, которая необходима для анализа. В ответ на запрос KSN присылает одно из следующих заключений:

- `0` – **В обработке**. Для получения заключения требуется отправить запрос повторно. Отправку повторных запросов вы можете настроить с помощью переключателя **Выполнять повторный запрос**.
- `1` – **Вредоносность не подтверждена**. На момент получения заключения библиотека не считается вредоносной.
- `2` – **Подозрительная**. При получении этого заключения создается алерт, если у вас настроено соответствующее правило корреляции.
- `3` – **Вредоносная**. При получении этого заключения создается алерт, если у вас настроено соответствующее правило корреляции. Заключение **Вредоносная** с большей вероятностью указывает на обнаружение DLL Hijacking, чем заключение **Подозрительная**.

Заключение записывается в событие в поле KL_AI_DLLHijackingCheckResult в виде числового значения и текстового пояснения.

Для использования обогащения типа **Проверка DLL Hijacking** ваша лицензия должна включать в себя модуль AI. Главному администратору также требуется принять дополнительное Положение о KSN в разделе **Kaspersky Security Network** (**Параметры** → **KUMA** → **Открыть параметры KUMA** → **Интеграции** → **AI-сервисы** → **Обнаружение атак DLL Hijacking**). Если в вашем экземпляре Kaspersky SIEM Cloud несколько Главных администраторов, достаточно, чтобы Положение о KSN принял любой из них.

Если лицензия отсутствует или срок действия лицензии с модулем AI истек:

- Невозможно создавать правила обогащения с типом **Проверка DLL Hijacking**. При этом ранее созданные правила остаются доступны для просмотра, а также в течение семи дней доступны для изменения.
- Поле KL_AI_DLLHijackingCheckResult остается доступным для просмотра. Также вы можете выполнять поиск и фильтрацию по этому полю.
- Коллекторы не отправляют запрос по ранее настроенным обогащениям типом **Проверка DLL Hijacking**.

Обнаружение атак DLL Hijacking с помощью обогащения событий в коррелляторе

Чтобы настроить обнаружение атак DLL Hijacking с помощью обогащения событий в коррелляторе:

1. В веб-консоли откройте раздел **Мониторинг** → **Ресурсы и сервисы** → **Корреляторы**.
2. Запустите создание коррелятора или откройте параметры существующего коррелятора.
3. В разделе **Обогащение** выполните следующие действия:
   a. Добавьте правило обогащения типа **Проверка DLL Hijacking**.
   b. В блоке **Параметры фильтра** выберите из списка фильтр **[OOTB] Events for DLLHijacking enrichment. Filter for correlator**. Если этот фильтр отсутствует в списке, импортируйте его из репозитория. Вы также можете настроить фильтр самостоятельно.
4. В разделе **Корреляция** создайте правило корреляции типа **simple** или типа **standard**. В правиле корреляции укажите поля, которые вы указали при добавлении обогащения. Если вы создали правило корреляции типа **simple**, поля должны быть перечислены в параметре **Наследуемые поля**. Для правила корреляции типа **standard** поля перечисляются в параметре **Группирующие поля**.

Если вы хотите настроить решение так, чтобы при получении заключений **Подозрительная** или **Вредоносная** создавался алерт, при создании правила корреляции типа **simple** или типа **standard** на вкладке **Селектор** укажите в параметрах фильтра два условия:

```
Создание алерта для заключения Подозрительная

KL_AI_DLLHijackingCheckResult = 2
```

```
Создание алерта для заключения Вредоносная

KL_AI_DLLHijackingCheckResult = 3
```

5. Сохраните настроенные параметры коррелятора.

Обнаружение атак DLL Hijacking с помощью обогащения событий в коллекторе

Не рекомендуется использовать обогащение типа **Проверка DLL Hijacking** в коллекторе. Это повышает нагрузку на службу KSN. Вместо этого привяжите обогащение этого типа к коррелятору.

Чтобы настроить обнаружение атак DLL Hijacking с помощью обогащения событий в коллекторе:

1. В веб-консоли откройте раздел **Мониторинг** → **Ресурсы и сервисы** → **Коллекторы**.
2. Запустите создание коллектора или откройте параметры существующего коллектора.
3. В разделе **Обогащение** выполните следующие действия:
   a. Добавьте правило обогащения типа **Проверка DLL Hijacking**.

      Убедитесь, что указанные вами поля заполняются при нормализации в коллекторе.

   b. В блоке **Параметры фильтра** выберите из списка фильтр **[OOTB] Events for DLLHijacking enrichment. Filter for collector**. Если этот фильтр отсутствует в списке, импортируйте его из репозитория. Вы также можете настроить фильтр самостоятельно.
4. Если вы хотите настроить решение так, чтобы при получении заключений **Подозрительная** или **Вредоносная** создавался алерт, создайте соответствующее правило корреляции типа **simple** или типа **standard**, **указав** на вкладке **Селектор** в параметрах фильтра следующие условия:

```
Создание алерта для заключения Подозрительная

KL_AI_DLLHijackingCheckResult = 2
```

```
Создание алерта для заключения Вредоносная

KL_AI_DLLHijackingCheckResult = 3
```

5. Сохраните настроенные параметры коллектора.

Обнаружение атак DLL Hijacking будет настроено. Если вы создали правило корреляции, то при получении заключений **Подозрительная** или **Вредоносная** будет создаваться алерт.

Управление активами

Активы представляют собой устройства и системы в организации, для которых поступают события безопасности. Это могут быть рабочие станции, серверы, сетевое оборудование, мобильные устройства и другие объекты инфраструктуры. Активы генерируют сетевой трафик при отправке и получении данных. Решение может быть настроено для отслеживания этой активности и создания базовых событий с четким указанием того, откуда исходит трафик и куда он направляется. В событии могут быть записаны исходные и целевые IP-адреса, а также DNS-имена. Если вы регистрируете актив с определенными параметрами (например, конкретным IP-адресом), формируется связь между этим активом и всеми событиями, в которых указаны эти параметры (например, с IP-адресом).

Активы рекомендуется регистрировать в Kaspersky SIEM Cloud, поскольку их использование позволяет формулировать четкие и универсальные правила корреляции для более эффективного анализа событий.

После добавления активов в Kaspersky SIEM Cloud их идентификаторы будут добавляться при обогащении событий. При анализе событий вы получите дополнительную информацию об устройствах и системах в организации.

Вы можете просматривать информацию об активах, искать активы по заданным критериям, редактировать их и удалять, а также экспортировать данные о них в CSV-файл.

Категории активов

Активы можно группировать активы по категориям. Это позволяет создать прозрачную структуру вашей сети, а также дает дополнительные возможности при работе с правилами корреляции. Например, можно создавать алерты более высокого уровня важности для активов из более критичной категории. По умолчанию все активы находятся в категории **Активы без категории**. Устройство можно добавить в несколько категорий.

Когда обрабатывается событие, к которому привязан актив, категория этого актива также принимается во внимание. Например, если вы присвоите высокий уровень важности определенной категории активов, то связанные с этими активами базовые события создадут корреляционные события с более высоким уровнем важности. Что приведет к появлению обнаружений с более высоким уровнем важности и, следовательно, более быстрой реакцией на такой алерт.

По умолчанию категориям активов присвоены следующие уровни важности: Низкий, Средний, Высокий, Критичный. Вы можете создать пользовательские категории и организовать вложенность.

Категории можно наполнять следующими способами:

- **Вручную**
- **Активно**: динамически, если актив соответствует условиям.

Условия активного наполнения

1. В раскрывающемся списке **Регулярность категоризации** укажите периодичность, с которой активы будут привязываться к категории. Можно выбрать значения от одного раза в час до одного раза в сутки.

   Категоризацию можно запустить принудительно, выбрав в контекстном меню категории **Начать категоризацию**.

2. В блоке параметров **Условия** укажите фильтр, которому должны соответствовать активы для привязывания к категории.

   Условия можно добавлять с помощью кнопок **Добавить условие**. Группы условий можно добавлять с помощью кнопок **Добавить группу**. Групповые операторы можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

   Операнды и операторы фильтра категоризации

Операнд	Операторы	Комментарий
Номер сборки	=, ilike	
ОС	=, ilike	Оператор **ilike** обеспечивает регистронезависимый поиск.
IP-адрес	inSubnet, inRange	IP-адрес указывается в нотации CIDR (например: 192.168.0.0/24). При выборе оператора inRange допускается указывать только адреса из частных диапазонов IP-адресов (например: 10.0.0.0-10.255.255.255). Оба адреса должны быть из одного диапазона.
Полное доменное имя	=, ilike	Оператор **ilike** обеспечивает регистронезависимый поиск.
CVE	=, in	Оператор **in** позволяет указать массив идентификаторов CVE (Common Vulnerabilities and Exposures), например, `CVE-2017-0143`.
CVSS	>, >=, =, <=,<	Уровень критичности уязвимостей CVE на активе. Возможные значения параметра CVSS – от 0 до 10. Для уязвимостей из Open Single Management Platform неприменимо.

Количество CVE	>, >=, =, <=, <	Количество уникальных уязвимостей с признаком CVE на активе. Уязвимости без CVE не учитываются.
		Для категоризации по количеству CVE с определенным уровнем критичности используется комбинированное условие. Например:
		`Количество CVE >= 1`
		И
		`CVSS >= 6.5`

ПО	=, ilike	Категоризация по ПО, установленному на активе. Оператор **ilike** обеспечивает регистронезависимый поиск.
Версия ПО	=, ilike, in	Категоризация по номеру версии (сборки) ПО, установленного на активе. Оператор **ilike** обеспечивает регистронезависимый поиск.
КИИ	in	Можно выбрать более одного значения.
Группа KSC	=, ilike	Категоризация по названию группы администрирования Open Single Management Platform, в которую помещен актив.
Последнее обновление антивирусных баз	>=,<=	Для выполнения категоризации время приводится в UTC, и затем в интерфейсе Kaspersky SIEM Cloud конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.

Последнее обновление информации	>=,<=	Для выполнения категоризации время приводится в UTC, и затем в интерфейсе Kaspersky SIEM Cloud конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Последнее обновление защиты	>=,<=	Для выполнения категоризации время приводится в UTC, и затем в интерфейсе Kaspersky SIEM Cloud конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Время начала последней сессии	>=,<=	Для выполнения категоризации время приводится в UTC, и затем в интерфейсе Kaspersky SIEM Cloud конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Расширенный статус KSC	in	Расширенный статус устройства. Можно выбрать более одного значения.
Статус постоянной защиты	=	Статус приложений "Лаборатории Касперского", установленных на управляемом устройстве.
Статус шифрования	=	
Статус защиты от спама	=	
Статус антивирусной защиты почтовых серверов	=	
Статус защиты данных от утечек	=	
Идентификатор расширенного статуса KSC	=	
Статус Endpoint Sensor	=	
Последнее появление в сети	>=,<=	Для выполнения категоризации время приводится в UTC, и затем в интерфейсе Kaspersky SIEM Cloud конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Рейтинг AI	>,>=,=,<=,<	Категоризация по рейтингам активов, присвоенным AI-сервисами.

Статус	=, in	Категоризация по предустановленным статусам актива, присвоенным AI-сервисами.
Настраиваемое поле актива	=, ilike	Категоризация по значениям настраиваемых полей активов.

Использование временных значений

Некоторые условия, например, **Последнее обновление антивирусных баз** или **Время начала последней сессии**, используют дату и время в качестве значения операнда. Для этих условий вы можете использовать точные дату и время или относительный период.

Чтобы указать значение даты и времени:

1. Выберите необходимый операнд, оператор и нажмите на поле даты.
2. Выполните одно из следующих действий:

   - В календаре выберите точную дату.

     По умолчанию к выбранной дате будет автоматически добавлено текущее время с точностью до миллисекунд. При изменении даты в календаре указанное время не меняется. Дата и время отображаются в соответствии с часовым поясом браузера. При необходимости вы можете изменить дату и время в поле вручную.

   - В списке **Относительный период** выберите относительный период.

     Период рассчитывается относительно текущего времени запуска категоризации и учитывает актуальную на этот момент информацию об активах. Например, для условия **Последнее обновление антивирусных баз** вы можете выбрать значение **1 час** и оператор **>=**, чтобы регулярно привязывать к категории активы, для которых антивирусные базы не обновлялись более 1 часа до запуска категоризации.

   - В поле даты и времени введите значение вручную.

     Вы можете указать точные дату и время в формате **DD.MM.YYYY HH:mm:ss.SSS** для русской локализации и **YYYY-MM-DD HH:mm:ss.SSS** для английской локализации или относительный период в виде формулы. При необходимости вы также можете комбинировать эти способы.

     Если при вводе точной даты вы не указали миллисекунды, значение 000 подставляется автоматически.

     В формулах относительного периода используйте параметр **now** для обозначения текущих даты и времени и язык параметризации интервалов: символы **+**, **-**, **/** (округление до ближайшего), а также единицы изменения времени **y** (год), **M** (месяц), **w** (неделя), **d** (день), **h** (час), **m** (минута), **s** (секунда).

     Например, для условия **Последнее обновление информации** вы можете указать значение **now-2d** с оператором **>=** и значение **now-1d** с оператором **>=**, чтобы регулярно привязывать к категории активы, информация о которых обновилась за сутки до запуска категоризации; или указать значение **now/w** с оператором **<=**, чтобы регулярно привязывать к категории активы, информация о которых обновилась с начала первого дня текущей недели (00:00:00:000 в UTC) до текущего времени **now**.

     Время в Kaspersky SIEM Cloud хранится в UTC, но в интерфейсе оно конвертируется в соответствии с часовым поясом вашего браузера. Это нужно учитывать для относительных периодов **Сегодня**, **Вчера**, **Эта неделя** и **Этот месяц**. Например, если в браузере установлен часовой пояс UTC+3 и вы выбрали период **Сегодня**, в категорию будут попадать активы за период с 03:00:00.000 до текущего времени, а не с 00:00:00.000.

Если при выборе относительного периода **Сегодня**, **Вчера**, **Эта неделя** или **Этот месяц** вы хотите при категоризации учитывать ваш часовой пояс, вам нужно вручную добавить сдвиг по времени в поле даты и времени, прибавив или убавив необходимое количество часов. Например, если в браузере установлен часовой пояс UTC+3 и вы хотите при категоризации учитывать период **Вчера**, вам нужно изменить значение на **now-1d/d-3h**. Если же вы хотите при категоризации учитывать период **Сегодня** – на **now/d-3h**.

3. С помощью кнопки **Проверить условия** убедитесь, что указанный фильтр верен: при нажатии на кнопку отображается окно **Активы, найденные по заданным условиям** с перечнем активов, удовлетворяющих условиям поиска.

Например, с момента перехода актива на указанную версию ОС или размещения актива в указанной подсети актив будет перемещен в заданную категорию. Если вы указали относительный период и выбрали регулярность категоризации, например, каждый час, при каждом запуске категоризации условие будет учитывать информацию об активах, актуальную на момент запуска категоризации.

- **Реактивно**: при срабатывания корреляционного правила актив будет перемещаться в указанную группу.

В Kaspersky SIEM Cloud активы распределены по тенантам и категориям. Активы выстроены в древовидную структуру, где в корне находятся тенанты и от них ветвятся категории активов. Вы можете просмотреть дерево тенантов и категорий в разделе **Управление активами → Управляемые устройства → Обнаружение и реагирование**. Если выбрать узел дерева, в правой части окна отображаются активы, относящиеся к соответствующей категории. Активы из подкатегорий выбранной категории отображаются, если вы укажете, что хотите отображать активы рекурсивно. Вы можете выделить флажками тенанты, активы которых хотите просматривать.

Чтобы вызвать контекстное меню категории, наведите указатель мыши на категорию и нажмите на значок с многоточием, который появится справа от названия категории. В контекстном меню доступны следующие действия:

Действия, доступные в контекстном меню категории

Действие	Описание
Показать активы	Просмотреть активы выбранной категории в правой части окна.
Отображать активы рекурсивно	Просмотреть активы из подкатегорий выбранной категории. Если вы хотите выйти из режима рекурсивного просмотра, выберите категорию для просмотра.
О категории	Просмотреть информации о выбранной категории в области деталей **Информация о категории**, которая отображается в правой части окна веб-интерфейса.
Начать категоризацию	Запустить автоматическое обновление активов в выбранной категории. В процессе обновления могут быть привязаны новые активы или исключены ранее привязанные. Доступно для категорий с активным способом категоризации.
Добавить подкатегорию	Добавить подкатегорию к выбранной категории.
Изменить категорию	Изменить выбранную категорию.
Удалить категорию	Удалить выбранную категорию. Удалять можно только категории без активов или подкатегорий. В противном случае опция **Удалить категорию** будет неактивна.
Сделать закладкой	Отобразить выбранную категорию на отдельной вкладке. Отменить это действие можно, выбрав в контекстном меню нужной категории **Убрать из закладок**.

Если вы хотите защитить более 10 000 активов (устройств), вам нужно отправить запрос в Службу технической поддержки "Лаборатории Касперского" и указать информацию о рабочей области, которую вы хотите создать.

Добавление категории активов

В Kaspersky SIEM Cloud вы можете добавить не более 1000 категорий активов.

Чтобы добавить категорию активов:

1. В OSMP Console перейдите в раздел **Управление активами → Управляемые устройства → Обнаружение и реагирование**.

   Наведите курсор на тенант, для которого хотите создать категорию, и нажмите на появившуюся кнопку +. Для создания подкатегории наведите курсор на родительскую категорию и нажмите на появившуюся кнопку +.

   В правой части окна консоли отобразится область деталей **Создать категорию**.

2. Добавьте сведения о категории:

   - В поле **Названия категорий** введите название категории. Название должно содержать от 1 до 128 символов в кодировке Unicode.

   - В поле **Родительская категория** отображается выбранная родительская категория.

     Вы можете изменить место категории в дереве категорий. Для этого разверните список категорий, нажав на иконку ⌄, и выберите желаемую родительскую категорию.

   - В поле **Тенант** отображается тенант, в структуре которого вы выбрали родительскую категорию. Тенант категории невозможно изменить.

   - В поле **Тип** выберите, как категория будет пополняться активами. В зависимости от выбора может потребоваться указать дополнительные параметры:

     - **Вручную** – активы можно привязать к категории только вручную.

     - **Активно** – активы будут с определенной периодичностью привязываться к категории, если удовлетворяют заданному фильтру.

       Активная категория активов

       1. В раскрывающемся списке **Регулярность категоризации** укажите периодичность, с которой активы будут привязываться к категории. Можно выбрать значения от одного раза в час до одного раза в сутки.

          Категоризацию можно запустить принудительно, выбрав в контекстном меню категории **Начать категоризацию**.

       2. В блоке параметров **Условия** укажите фильтр, которому должны соответствовать активы для привязывания к категории.

          Условия можно добавлять с помощью кнопок **Добавить условие**. Группы условий можно добавлять с помощью кнопок **Добавить группу**. Групповые операторы можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

          Операнды и операторы фильтра категоризации

Операнд	Операторы	Комментарий
Номер сборки	=, ilike	

ОС	=, ilike	Оператор **ilike** обеспечивает регистронезависимый поиск.
IP-адрес	inSubnet, inRange	IP-адрес указывается в нотации CIDR (например: 192.168.0.0/24). При выборе оператора inRange допускается указывать только адреса из частных диапазонов IP-адресов (например: 10.0.0.0-10.255.255.255). Оба адреса должны быть из одного диапазона.
Полное доменное имя	=, ilike	Оператор **ilike** обеспечивает регистронезависимый поиск.
CVE	=, in	Оператор **in** позволяет указать массив идентификаторов CVE (Common Vulnerabilities and Exposures), например, `CVE-2017-0143`.
CVSS	>, >=, =, <=,<	Уровень критичности уязвимостей CVE на активе. Возможные значения параметра CVSS – от 0 до 10. Для уязвимостей из Open Single Management Platform неприменимо.

Количество CVE	>, >=, =, <=, <	Количество уникальных уязвимостей с признаком CVE на активе. Уязвимости без CVE не учитываются.
		Для категоризации по количеству CVE с определенным уровнем критичности используется комбинированное условие. Например:
		`Количество CVE >= 1`
		И
		`CVSS >= 6.5`

ПО	=, ilike	Категоризация по ПО, установленному на активе. Оператор **ilike** обеспечивает регистронезависимый поиск.
Версия ПО	=, ilike, in	Категоризация по номеру версии (сборки) ПО, установленного на активе. Оператор **ilike** обеспечивает регистронезависимый поиск.
КИИ	in	Можно выбрать более одного значения.
Группа KSC	=, ilike	Категоризация по названию группы администрирования Open Single Management Platform, в которую помещен актив.
Последнее обновление антивирусных баз	>=,<=	Для выполнения категоризации время приводится в UTC, и затем в интерфейсе Kaspersky SIEM Cloud конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Последнее обновление информации	>=,<=	Для выполнения категоризации время приводится в UTC, и затем в интерфейсе Kaspersky SIEM Cloud конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.

Последнее обновление защиты	>=,<=	Для выполнения категоризации время приводится в UTC, и затем в интерфейсе Kaspersky SIEM Cloud конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Время начала последней сессии	>=,<=	Для выполнения категоризации время приводится в UTC, и затем в интерфейсе Kaspersky SIEM Cloud конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Расширенный статус KSC	in	Расширенный статус устройства. Можно выбрать более одного значения.
Статус постоянной защиты	=	Статус приложений "Лаборатории Касперского", установленных на управляемом устройстве.
Статус шифрования	=	
Статус защиты от спама	=	
Статус антивирусной защиты почтовых серверов	=	
Статус защиты данных от утечек	=	
Идентификатор расширенного статуса KSC	=	
Статус Endpoint Sensor	=	
Последнее появление в сети	>=,<=	Для выполнения категоризации время приводится в UTC, и затем в интерфейсе Kaspersky SIEM Cloud конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*. Использование относительного периода при регулярной категоризации учитывает актуальную на момент запуска категоризации информацию об активах.
Рейтинг AI	>,>=,=,<=,<	Категоризация по рейтингам активов, присвоенным AI-сервисами.
Статус	=, in	Категоризация по предустановленным статусам актива, присвоенным AI-сервисами.
Настраиваемое поле актива	=, ilike	Категоризация по значениям настраиваемых полей активов.

Использование временных значений

Некоторые условия, например, **Последнее обновление антивирусных баз** или **Время начала последней сессии**, используют дату и время в качестве значения операнда. Для этих условий вы можете использовать точные дату и время или относительный период.

Чтобы указать значение даты и времени:

1. Выберите необходимый операнд, оператор и нажмите на поле даты.

2. Выполните одно из следующих действий:

   - В календаре выберите точную дату.

     По умолчанию к выбранной дате будет автоматически добавлено текущее время с точностью до миллисекунд. При изменении даты в календаре указанное время не меняется. Дата и время отображаются в соответствии с часовым поясом браузера. При необходимости вы можете изменить дату и время в поле вручную.

   - В списке **Относительный период** выберите относительный период.

     Период рассчитывается относительно текущего времени запуска категоризации и учитывает актуальную на этот момент информацию об активах. Например, для условия **Последнее обновление антивирусных баз** вы можете выбрать значение **1 час** и оператор **>=**, чтобы регулярно привязывать к категории активы, для которых антивирусные базы не обновлялись более 1 часа до запуска категоризации.

   - В поле даты и времени введите значение вручную.

     Вы можете указать точные дату и время в формате **DD.MM.YYYY HH:mm:ss.SSS** для русской локализации и **YYYY-MM-DD HH:mm:ss.SSS** для английской локализации или относительный период в виде формулы. При необходимости вы также можете комбинировать эти способы.

     Если при вводе точной даты вы не указали миллисекунды, значение 000 подставляется автоматически.

     В формулах относительного периода используйте параметр **now** для обозначения текущих даты и времени и язык параметризации интервалов: символы **+**, **-**, **/** (округление до ближайшего), а также единицы изменения времени **y** (год), **M** (месяц), **w** (неделя), **d** (день), **h** (час), **m** (минута), **s** (секунда).

     Например, для условия **Последнее обновление информации** вы можете указать значение **now-2d** с оператором **>=** и значение **now-1d** с оператором **>=**, чтобы регулярно привязывать к категории активы, информация о которых обновилась за сутки до запуска категоризации; или указать значение **now/w** с оператором **<=**, чтобы регулярно привязывать к категории активы, информация о которых обновилась с начала первого дня текущей недели (00:00:00:000 в UTC) до текущего времени **now**.

     Время в Kaspersky SIEM Cloud хранится в UTC, но в интерфейсе оно конвертируется в соответствии с часовым поясом вашего браузера. Это нужно учитывать для относительных периодов **Сегодня**, **Вчера**, **Эта неделя** и **Этот месяц**. Например, если в браузере установлен часовой пояс UTC+3 и вы выбрали период **Сегодня**, в категорию будут попадать активы за период с 03:00:00.000 до текущего времени, а не с 00:00:00.000.

Если при выборе относительного периода **Сегодня**, **Вчера**, **Эта неделя** или **Этот месяц** вы хотите при категоризации учитывать ваш часовой пояс, вам нужно вручную добавить сдвиг по времени в поле даты и времени, прибавив или убавив необходимое количество часов. Например, если в браузере установлен часовой пояс UTC+3 и вы хотите при категоризации учитывать период **Вчера**, вам нужно изменить значение на **now-1d/d-3h**. Если же вы хотите при категоризации учитывать период **Сегодня** – на **now/d-3h**.

3. С помощью кнопки **Проверить условия** убедитесь, что указанный фильтр верен: при нажатии на кнопку отображается окно **Активы, найденные по заданным условиям** с перечнем активов, удовлетворяющих условиям поиска.

- **Реактивно** – категория будет наполняться активами с помощью правил корреляции.

- Назначьте уровень важности категории в поле **Важность**.

- При необходимости в поле **Описание** добавьте примечание: до 256 символов в кодировке Unicode.

3. Нажмите на кнопку **Создать**.

Новая категория добавлена в дерево категорий активов.

Настройка таблицы активов

В OSMP Console можно настроить содержимое и порядок отображения столбцов в таблице активов. Эти параметры хранятся локально на вашем компьютере.

Чтобы настроить параметры отображения таблицы активов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства** → **Обнаружение и реагирование**.

2. В правом верхнем углу таблицы активов нажмите на значок **Параметры** (⚙).

3. В раскрывшемся списке установите флажки напротив параметров, которые требуется отображать в таблице:

- **Имя**
- **FQDN**
- **IP-адрес**
- **Категории**
- **MAC-адрес**
- **Источник актива**
- **ОС**
- **Создано**
- **Обновлено**

- **КИИ-категория**
- **Отправлено в архив** – когда флажок установлен и столбец отображается в таблице активов, в раскрывающемся списке в столбце **Отправлено в архив** доступны следующие параметры фильтрации активов:
  - **Да** – отображаются только активы в архивах.
  - **Нет** – отображаются только действующие активы.
- **Вес**
- **Группа администрирования**
- **Телеметрия получена**
- **Статус телеметрии**
- **Статус EDR**
- **Последнее подключение к KSC**
- **Последнее подключение к EDR**
- **Лицензия EDR**
- **Версия агента EDR**
- **Статус изоляции**
- **Владелец**
- **Адрес**

Когда вы устанавливаете флажок, таблица активов обновляется и добавляется новый столбец. При снятии флажка столбец исчезает. Таблицу можно сортировать по некоторым столбцам.

4. Если требуется изменить порядок отображения столбцов, зажмите левую клавишу мыши на названии столбца и перетащите его в нужное место таблицы.

Параметры отображения таблицы активов настроены.

Поиск активов

В OSMP Console есть два режима поиска активов. Переключение между режимами поиска осуществляется с помощью кнопок в верхней левой части окна:

- – простой поиск по параметрам активов **Имя**, **FQDN**, **IP-адрес**, **MAC-адрес** и **Владелец**.
- – сложный поиск активов с помощью фильтрации по условиям и группам условий.

Найденные активы можно выделить, установив напротив них флажки, и экспортировать данные о них в виде CSV-файла.

Простой поиск

Чтобы найти актив с помощью простого поиска,

в разделе **Управление активами** → **Управляемые устройства** → **Обнаружение и реагирование** введите поисковый запрос в поле **Поиск**.

В таблице отобразятся активы, у которых параметры **Имя**, **FQDN**, **IP-адрес**, **MAC-адрес** и **Владелец** соответствуют критериям поиска.

Сложный поиск

Чтобы найти актив с помощью сложного поиска:

1. В разделе **Управление активами** → **Управляемые устройства** → **Обнаружение и реагирование** нажмите на значок воронки ( ).

   В верхней части окна отображается блок настройки фильтрации активов.

2. Задайте параметры фильтрации активов и нажмите на кнопку **Поиск**.

   Подробнее о параметрах фильтрации активов см. в таблице ниже.

В таблице отобразятся активы, которые соответствуют критериям поиска.

Сложный поиск активов производится с помощью условий фильтрации, которые можно задать в верхней части окна:

- С помощью кнопки **Добавить условие** можно добавить строку с полями для определения условия.
- С помощью кнопки **Добавить группу** можно добавить группу фильтров. Можно переключать групповые операторы между **И**, **ИЛИ**, **НЕ**.
- Условия и группы условий можно перетягивать мышкой.
- Условия, группы и фильтры можно удалить с помощью кнопки ×.
- Параметры фильтрации можно обнулить с помощью кнопки **Очистить все**.
- Операторы условий и доступные значения правого операнда зависят от выбранного левого операнда:

Левый операнд	Доступные операторы	Правый операнд
Номер сборки	=, ilike	Произвольное значение.
ОС	=, ilike	Произвольное значение.
IP-адрес	inSubnet, inRange	Произвольное значение или диапазон значений. Условие фильтрации для оператора inSubnet выполнится, если IP-адрес, который содержится в левом операнде входит в подсеть, которая указан в правом операнде. Например, для IP-адреса 10.80.16.206 в правом операнде следует указать подсеть в короткой нотации: `10.80.16.206/25`.
Полное доменное имя	=, ilike	Произвольное значение.

CVE	=, in	Произвольное значение. Оператор **in** позволяет указать массив идентификаторов CVE (Common Vulnerabilities and Exposures), например, `CVE-2017-0143`.
CVSS	>, >=, =, <=, <	Число от 0 до 10 (возможные значения уровня критичности уязвимости CVE на активе). Для уязвимостей из Open Single Management Platform неприменимо.

Количество CVE	>, >=, =, <=, <	Число. Количество уникальных уязвимостей с признаком CVE на активе. Уязвимости без CVE не учитываются.
		Если в качестве правого операнда указано значение `0` и выбран оператор `=` или `<=`, в результатах поиска будут отображаться активы, у которых отсутствуют уязвимости с CVE.
		Для поиска по количеству CVE с определенным уровнем критичности используется комбинированное условие. Например:
		`Количество CVE >= 1`
		`CVSS >= 6.5`

ПО	=, ilike	Произвольное значение.
Версия ПО	=, ilike, in	Произвольное значение. Номер версии (сборки) ПО, установленного на активе.
Источник актива	in	• Open Single Management Platform. • KICS/KATA. • Создан вручную.
КИИ	in	• Информационный ресурс не является объектом КИИ. • Объект КИИ без категории значимости. • Объект КИИ третьей категории значимости. • Объект КИИ второй категории значимости. • Объект КИИ первой категории значимости.
ОЗУ (байтов)	=, >, >=, <, <=	Число.
Количество дисков	=, >, >=, <, <=	Число.
Количество сетевых карт	=, >, >=, <, <=	Число.
Свободных байт на диске	=, >, >=, <, <=	Число.
Группа KSC	=, ilike	Произвольное значение. Название группы администрирования Open Single Management Platform, в которую помещен актив.
Последнее обновление антивирусных баз	>=, <=	Для поиска время приводится в UTC, и затем в интерфейсе Kaspersky SIEM Cloud конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*.
Последнее обновление информации	>=, <=	Для поиска время приводится в UTC, и затем в интерфейсе Kaspersky SIEM Cloud конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*.
Последнее обновление защиты	>=, <=	Для поиска время приводится в UTC, и затем в интерфейсе Kaspersky SIEM Cloud конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*.

Время начала последнего сеанса	>=, <=	Для поиска время приводится в UTC, и затем в интерфейсе Kaspersky SIEM Cloud конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*.
Расширенный статус KSC	in	• Устройство с установленным Агентом администрирования подключено к сети, но Агент администрирования неактивен. • Антивирусное приложение установлено, но постоянная защита не работает. • Антивирусное приложение установлено, но не запущено. • Количество обнаруженных вирусов слишком велико. • Антивирусное приложение установлено, но статус постоянной защиты отличается от установленного администратором безопасности. • Антивирусное приложение не установлено. • Полная проверка на вирусы выполнялась слишком давно. • Антивирусные базы обновлялись слишком давно. • Агент администрирования слишком долго был неактивен. • Устаревшая лицензия. • Количество невылеченных объектов слишком велико. • Требуется перезагрузка. • На устройстве установлено одно или несколько несовместимых приложений. • Устройство имеет одну или несколько уязвимостей. • Последний поиск обновлений операционной системы на устройстве выполнялся слишком давно. • Устройство не имеет надлежащего статуса шифрования. • Параметры мобильного устройства не соответствуют требованиям политики безопасности. • Есть необработанные инциденты. • Статус устройства был предложен управляемым приложением. • На устройстве недостаточно места на диске: возникают ошибки синхронизации или на диске недостаточно места.
Статус постоянной защиты	=	• Неизвестно. • Остановлена. • Приостановлена. • Запускается. • Выполняется (если антивирусное приложение не поддерживает категории состояния Выполняется). • Выполняется с максимальной защитой. • Выполняется с максимальным быстродействием. • Выполняется с рекомендуемыми параметрами. • Выполняется с пользовательскими параметрами. • Ошибка.
Статус шифрования	=	• На устройстве нет правил шифрования. • Шифрование выполняется. • Шифрование отменено пользователем. • Во время шифрования произошла ошибка. • Все правила шифрования устройства были выполнены. • Шифрование выполняется, на устройстве требуется перезагрузка. • На устройстве есть зашифрованные файлы без указанных правил шифрования.
Статус защиты от спама	=	• Неизвестно. • Остановлена. • Приостановлена. • Запускается. • Выполняется. • Ошибка. • Не установлено. • Лицензия отсутствует.
Статус антивирусной защиты почтовых серверов	=	• Неизвестно. • Остановлена. • Приостановлена. • Запускается. • Выполняется. • Ошибка. • Не установлено. • Лицензия отсутствует.
Статус защиты данных от утечек	=	• Неизвестно. • Остановлена. • Приостановлена. • Запускается. • Выполняется.

		• Ошибка. • Не установлено. • Лицензия отсутствует.
Идентификатор расширенного статуса KSC	=	• OK. • Критический. • Требует внимания.
Статус Endpoint Sensor	=	• Неизвестно. • Остановлена. • Приостановлена. • Запускается. • Выполняется. • Ошибка. • Не установлено. • Лицензия отсутствует.
Последнее появление в сети	>=, <=	Для поиска время приводится в UTC, и затем в интерфейсе Kaspersky SIEM Cloud конвертируется в соответствии с локальным часовым поясом, установленным в браузере. Вы можете указать дату и время для этого операнда одним из следующих способов: • Выбрать точную дату в календаре. • Выбрать период относительно настоящего времени в списке **Относительный период**. • Указать значение вручную: точные дату и время или относительный период, а также комбинацию этих способов. Подробнее см. ниже в подразделе *Использование временных значений*.
Рейтинг AI	=, >, >=, <, <=	Число. Рейтинг активов, присвоенный AI-сервисами.
Статус	=, in	Статусы активов, присвоенные AI-сервисами: • Низкий. • Средний. • Высокий. • Критический.
Настраиваемое поле актива	=, ilike	Произвольное значение. Поиск по настраиваемым полям активов.

Использование временных значений

Некоторые условия, например, **Последнее обновление антивирусных баз** или **Время начала последней сессии**, используют дату и время в качестве значения операнда. Для этих условий вы можете использовать точные дату и время или относительный период.

Чтобы указать значение даты и времени:

1. Выберите необходимый операнд, оператор и нажмите на поле даты.
2. Выполните одно из следующих действий:
   - В календаре выберите точную дату.

     По умолчанию к выбранной дате будет автоматически добавлено текущее время с точностью до миллисекунд. При изменении даты в календаре указанное время не меняется. Дата и время отображаются в соответствии с часовым поясом браузера. При необходимости вы можете изменить дату и время в поле вручную.
   - В списке **Относительный период** выберите относительный период.

     Период рассчитывается относительно текущего времени поиска и учитывает актуальную на этот момент информацию об активах. Например, для условия **Последнее обновление антивирусных баз** вы можете выбрать значение **1 час** и оператор **>=**, чтобы найти активы, для которых антивирусные базы не обновлялись более 1 часа.
   - В поле даты и времени введите значение вручную.

Вы можете указать точные дату и время в формате **DD.MM.YYYY HH:mm:ss.SSS** для русской локализации и **YYYY-MM-DD HH:mm:ss.SSS** для английской локализации или относительный период в виде формулы. При необходимости вы также можете комбинировать эти способы.

Если при вводе точной даты вы не указали миллисекунды, значение 000 подставляется автоматически.

В формулах относительного периода используйте параметр **now** для обозначения текущих даты и времени и язык параметризации интервалов: символы **+**, **-**, **/** (округление до ближайшего), а также единицы изменения времени **y** (год), **M** (месяц), **w** (неделя), **d** (день), **h** (час), **m** (минута), **s** (секунда).

Например, для условия **Последнее обновление информации** вы можете указать значение **now-2d** с оператором **>=** и значение **now-1d** с оператором **>=**, чтобы найти активы, информация о которых обновилась за сутки до запуска поиска; или указать значение **now/w** с оператором **<=**, чтобы найти активы, информация о которых обновилась с начала первого дня текущей недели (00:00:00:000 в UTC) до текущего времени **now**.

Время в Kaspersky SIEM Cloud хранится в UTC, но в интерфейсе оно конвертируется в соответствии с часовым поясом вашего браузера. Это нужно учитывать для относительных периодов **Сегодня**, **Вчера**, **Эта неделя** и **Этот месяц**. Например, если в браузере установлен часовой пояс UTC+3 и вы выбрали период **Сегодня**, в категорию будут попадать активы за период с 03:00:00.000 до текущего времени, а не с 00:00:00.000.

Если при выборе относительного периода **Сегодня**, **Вчера**, **Эта неделя** или **Этот месяц** вы хотите при категоризации учитывать ваш часовой пояс, вам нужно вручную добавить сдвиг по времени в поле даты и времени, прибавив или убавив необходимое количество часов. Например, если в браузере установлен часовой пояс UTC+3 и вы хотите при категоризации учитывать период **Вчера**, вам нужно изменить значение на **now-1d/d-3h**. Если же вы хотите при категоризации учитывать период **Сегодня** – на **now/d-3h**.

Экспорт данных об активах

Данные об активах, отображаемых в таблице активов, можно экспортировать в виде CSV-файла.

Чтобы экспортировать данные об активах:

1. Настройте таблицу активов.

   В файл записываются только данные, указанные в таблице. Порядок отображения столбцов таблицы активов повторяется в экспортированном файле.

2. Найдите нужные активы и выберите их, установив рядом с ними флажки.

   При необходимости вы можете выбрать сразу все активы в таблице, установив флажок в левой части заголовка таблицы активов.

3. В панели инструментов или в меню ⋮ нажмите на кнопку **Экспортировать в CSV**.

Данные об активах будут записаны в файл assets_<дата экспорта>_<время экспорта>.csv. Файл будет скачан в соответствии с параметрами вашего браузера.

Просмотр информации об активе

Чтобы просмотреть информацию об активе, откройте окно информации об активе одним из следующих способов:

- В веб-консоли перейдите в раздел **Управление активами** → **Управляемые устройства**, выберите категорию с нужными активами и выберите актив.
- В веб-консоли перейдите в раздел **Мониторинг** → **Алерты** → нажмите на ссылку с требуемым алертом → в разделе **Связанные активы** выберите актив.
- В веб-консоли перейдите в раздел **Мониторинг** → **Поиск угроз**→ выполните поиск и фильтрацию событий → выберите нужное событие → нажмите на ссылку в одном из следующих полей: SourceAssetID, DestinationAssetID или DeviceAssetID.

В окне информации об активе может отображаться следующая информация:

- **Название, ID** – имя актива, идентификатор.

  Активы, импортированные в OSMP Console, сохраняют имена, которые были заданы для них в источнике. Вы можете изменить имена активов в веб-интерфейсе OSMP Console.
- **Тенант** – название тенанта, которому принадлежит актив.
- **Отправлено в архив** – статус архивации актива. Доступные значения: Да, Нет.
- **Источник актива** – источник информации об активе. Источников может быть несколько: сведения можно добавить в веб-интерфейсе OSMP Console или с помощью API, а также импортировать из Open Single Management Platform и KICS/KATA.

  Добавляя в OSMP Console сведения об одном и том же активе из нескольких источников, следует учитывать правила слияния данных об активах.
- **Создано** – дата и время добавления актива в OSMP Console.
- **Обновлено** – дата и время изменения информации об активе.
- **Владелец** – владелец актива, если он указан.
- **IP-адрес** – IP-адрес актива (если есть).

  > Если в OSMP Console есть несколько активов с одинаковыми IP-адресами, актив, добавленный позже, возвращается во всех случаях поиска активов по IP-адресу. Если в сети вашей организации допустимо наличие активов с одинаковыми IP-адресами, разработайте и используйте дополнительные атрибуты для идентификации активов. Это может оказаться важным при корреляции.
- **FQDN** – полностью определенное имя домена актива, если указано.
- **MAC-адрес** – MAC-адрес актива (если есть).
- **Название ОС** – операционная система актива.

- **Связанные алерты** – алерты, с которыми связан актив (если есть).

  Для просмотра списка алертов, с которыми связан актив, можно перейти по ссылке **Найти в алертах**. Откроется вкладка **Алерты** с поисковым выражением, позволяющим отфильтровать все активы с соответствующим идентификатором.

- **Настраиваемые поля** – данные, записанные в настраиваемые поля активов.

- **Категории** – категории, к которым относится актив (если есть).

- По кнопке **Реагирование** → **Переместить в группу** вы можете переместить просматриваемый актив между группами администрирования Open Single Management Platform.

Добавление активов

Вы можете добавлять информацию об активах следующими способами:

- Вручную.

  Вы можете добавить актив в Консоли OSMP или с помощью API.

- Импортировать активы.

  Вы можете импортировать активы из Kaspersky Security Center, KICS for Networks и MaxPatrol VM.

При добавлении активы, уже существующие в OSMP, могут объединяться с добавляемыми активами.

Алгоритм объединения активов:

1. Проверка на уникальность активов в Kaspersky Security Center или KICS for Networks активов:

   - Уникальность актива импортированного из Kaspersky Security Center, проверяется по параметру **Идентификатор устройства**, в котором указан идентификатор *агента администрирования* Kaspersky Security Center. Если идентификаторы у двух активов различаются, активы считаются разными, объединения данных не происходит.

   - Уникальность актива импортированного из KICS for Networks, определяется по комбинации параметров **IP-адрес**, **IP-адрес сервера KICS for Networks** и **Идентификатор коннектора KICS for Networks**. Если любой из параметров у двух активов различается, активы считаются разными, объединения данных не происходит.

   Если активы совпадают, алгоритм выполняется далее.

2. Проверка на совпадение значений в полях **IP**, **MAC**, **FQDN**.

   Если хотя бы два из указанных полей совпадают, активы объединяются при условии, что другие поля не заполнены.

   Возможные варианты совпадений:

   - FQDN и IP-адрес активов. Поле **MAC** не заполнено.

     Проверка производится по всему массиву значений IP-адресов. Если IP-адрес актива входит в состав FQDN, значения считаются совпавшими.

   - FQDN и MAC-адрес активов. Поле **IP** не заполнено.

     Проверка производится по всему массиву значений MAC-адресов. При полном совпадении хотя бы одного значения массива с FQDN значения считаются совпавшими.

- IP-адрес и MAC-адрес активов. Поле **FQDN** не заполнено.

  Проверка производится по всему массиву значений IP- и MAC-адресов. При полном совпадении хотя бы одного значения в массивах значения считаются совпавшими.

3. Проверка на совпадение хотя бы одного из полей **IP**, **MAC**, **FQDN** при условии, что два других поля не заполнены для одного или обоих активов.

   Активы объединяются, если значения в поле совпадают. Например, если для актива KUMA указаны FQDN и IP-адрес, а для импортируемого актива только IP-адрес с тем же значением, поля считаются совпавшими. В этом случае активы объединяются.

   Для каждого поля проверка производится отдельно и завершается при первом совпадении.

Вы можете посмотреть примеры сравнения полей активов здесь.

Информация об активах может формироваться из разных источников. Если добавляемый актив и актив OSMP содержат данные, полученные из одного и того же источника, эти данные перезаписываются. Например, актив Kaspersky Security Center при импорте в OSMP получил полное доменное имя и информацию о программном обеспечении. При импорте актива из Kaspersky Security Center с аналогичным полным доменным именем эти данные будут перезаписаны при условии, что они указаны для добавляемого актива. Все поля, в которых могут обновляться данные, приведены в таблице Обновляемые данные.

Обновляемые данные

Название поля	Принцип обновления
Имя	Выбирается согласно следующему приоритету: • Задано вручную. • Получено из Kaspersky Security Center. • Получено KICS for Networks.
Владелец	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Задано вручную.
IP-адрес;	Данные объединяются. Если в массиве адресов есть одинаковые адреса, копия дублирующегося адреса удаляется.
FQDN	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Получено KICS for Networks. • Задано вручную.
MAC-адрес	Данные объединяются. Если в массиве адресов есть одинаковые адреса, один из дублирующихся адресов удаляется.
Операционная система	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Получено KICS for Networks. • Задано вручную.
Уязвимости	Данные активов KUMA дополняются информацией из добавляемых активов. В информации об активе данные группируются по названию источника. Устранение уязвимостей для каждого источника осуществляется отдельно.
Информация о программном обеспечении	Данные из KICS for Networks записываются всегда (при наличии). Для других источников выбирается первое значение согласно следующему приоритету: • Получено из Kaspersky Security Center. • Задано вручную.

Название поля	Принцип обновления
Информация об оборудовании	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Задано через API.

Обновленные данные отображаются в информации об активе. Вы можете просмотреть информацию об активе в Консоли OSMP.

При добавлении новых активов эти данные могут быть перезаписаны. Если данные, из которых сформирована информация об активе, не обновляются из источников более 30 дней, актив удаляется. При следующем добавлении актива из тех же источников создается новый актив.

При изменении в Консоли OSMP активов, информация о которых получена из Kaspersky Security Center или KICS for Networks, вы можете изменить следующие данные актива:

- Название.
- Категория.

Если информация об активе добавлена вручную, при редактировании в Консоли OSMP этих активов вы можете изменить следующие данные актива:

- Название.
- Название тенанта, которому принадлежит актив.
- IP-адрес.
- Полное доменное имя.
- MAC-адрес.
- Владелец.
- Категория.
- Операционная система.
- Информация об оборудовании.

Редактирование данных об активах через REST API недоступно. При импорте из REST API происходит обновление данных по правилам слияния информации об активах, приведенным выше.

Добавление информации об активах

Чтобы добавить актив в OSMP Console:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства** → **Обнаружение и реагирование** и нажмите **Добавить**.

   В правой части окна откроется область деталей **Добавить актив**.

2. Введите параметры актива:

   - **Имя актива** (обязательно).
   - **IP-адрес** и/или **FQDN** (обязательно). Вы можете указать несколько FQDN, нажав на кнопку **Добавить FQDN**.
   - **MAC-адрес.**
   - **Владелец.**

3. При необходимости заполните параметры на следующих вкладках:

   - **Дополнительно** — сведения о владельце, категории, операционной системе актива.
   - **Оборудование** — сведения об оборудовании актива.

4. Нажмите на кнопку **Добавить**.

   Актив создан и отображается в таблице активов в назначенной ему категории или в категории **Активы без категории**.

Импорт информации об активах из Kaspersky Security Center

В Kaspersky Security Center зарегистрированы все активы, которые находятся под защитой этого приложения. Вы можете импортировать информацию об активах, защищаемых Kaspersky Security Center, в KUMA. Для этого вам требуется предварительно настроить интеграцию между приложениями.

Kaspersky SIEM Cloud импортирует следующие данные об устройстве, полученные от Агентов администрирования Kaspersky Security Center:

- основную информацию об активе – имя, адрес, время подключения к Kaspersky Security Center, информацию об оборудовании, состоянии защиты, версии антивирусных баз;
- информацию об атрибутах актива – об уязвимостях, о программном обеспечении, включая операционную систему, о владельцах.

Чтобы импортировать информацию об активах Kaspersky Security Center:

1. В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства → Обнаружение и реагирование**.

2. Нажмите **Импортировать** и выберите одно из следующих действий:

   - Чтобы импортировать информацию об основных атрибутах активов, нажмите **Импортировать активы KSC**.

     Откроется окно **Импорт активов KSC**.

   - Чтобы импортировать информацию о других атрибутах активов, нажмите **Импортировать атрибуты активов KSC**.

     Откроется окно **Импортировать атрибуты активов KSC**.

3. В раскрывающемся списке выберите тенант, для которого вы хотите выполнить импорт.

В этом случае приложение загружает информацию обо всех активах всех Серверов администрирования Kaspersky Security Center, для которых настроено подключение к выбранному тенанту.

Если вы хотите импортировать информацию обо всех активах всех Серверов администрирования Kaspersky Security Center для всех тенантов, выберите **Все**.

4. Нажмите на кнопку **Импортировать**.

Информация об активах будет импортирована.

Также в окне свойств тенанта вы можете настроить периодический импорт информации об активах или запустить импорт вручную.

Импорт информации об активах из MaxPatrol

Вы можете импортировать в XDR сведения об активах из системы MaxPatrol VM. Импортированные активы отображаются в группе **Активы**. При необходимости вы можете редактировать параметры активов.

Импорт информации об активах из MaxPatrol VM

Дистрибутив OSMP включает утилиту kuma-ptvm, которая состоит из исполняемого файла и конфигурационного файла. Утилита поддерживает операционные системы Windows и Linux. Утилита позволяет подключаться к API MaxPatrol VM для получения данных об устройствах и их атрибутах, включая уязвимости, а также позволяет изменять данные активов и импортировать данные с использованием API Kaspersky Symphony XDR. Импорт данных поддерживается для MaxPatrol VM версий 1.1–2.7 включительно.

Настройка импорта информации об активе из MaxPatrol VM в Ядро Kaspersky SIEM Cloud включает следующие этапы:

1. Подготовка Kaspersky Symphony XDR и MaxPatrol VM.

   Вам нужно создать учетные записи пользователей и токен Kaspersky Symphony XDR для операций API.

2. Создание конфигурационного файла с параметрами экспорта и импорта данных.

3. Импорт данных активов в Ядро Kaspersky SIEM Cloud с использованием утилиты kuma-ptvm:

   a. Данные экспортируются из MaxPatrol VM и сохраняются в директории утилиты.

      При необходимости вы можете изменить полученные файлы.

   b. Информация из файлов импортируется в Ядро Kaspersky SIEM Cloud.

При повторном импорте существующих активов, активы, которые уже существуют в Ядре Kaspersky SIEM Cloud, перезаписываются. Таким образом закрытые уязвимости будут удалены.

Известные ограничения:

- Если один и тот же IP-адрес указан для двух активов с разными FQDN, Ядро Kaspersky SIEM Cloud импортирует такие активы как два разных актива. Эти активы не объединяются.

- Если на активе установлено два приложения с одинаковыми данными в полях названия, версии и поставщика, Ядро Kaspersky SIEM Cloud импортирует эти данные как одно приложение, несмотря на разные пути установки приложения на активе.

- Если FQDN актива содержит пробел или подчеркивание (_), данные таких активов не импортируются в Ядро Kaspersky SIEM Cloud. В журнале событий будет указано, что активы были пропущены при импорте.
- Если во время импорта происходит ошибка, сведения об ошибке регистрируются и импорт останавливается.

Подготовительные действия:

1. Создайте отдельную учетную запись в Kaspersky Symphony XDR и в MaxPatrol VM с минимально необходимым набором разрешений для использования API запросов.
2. Создайте учетные записи пользователей, для которых вы позже сгенерируете токен API.

   Требования к учетным записям, для которых генерируется API-токен:

   - Главный администратор, Администратор тенанта, Аналитик 2-го уровня или Аналитик 1-го уровня.
   - В учетной записи пользователя, в разделе прав доступа к API, установлен флажок для POST /xdr/api/v2.1/kuma/assets/import.
3. Сгенерировать токен для доступа к XDR REST API.
4. Скопируйте утилиту kuma-ptvm на сервер с Ядром Kaspersky SIEM Cloud и сделайте файл утилиты исполняемым с помощью команды:

   ```
   chmod +x <путь до файла kuma-ptvm на сервере с Ядром Kaspersky SIEM Cloud>
   ```

Чтобы создать конфигурационный файл:

1. Перейдите в папку утилит Kaspersky SIEM Cloud:

   ```
   cd /opt/kaspersky/kuma/utils/
   ```

2. Скопируйте шаблон kuma-ptvm-config-template.yaml, чтобы создать конфигурационный файл с именем kuma-ptvm-config.yaml.

   ```
   cp kuma-ptvm-config-template.yaml kuma-ptvm-config.yaml
   ```

3. Измените параметры в конфигурационном файле kuma-ptvm-config.yaml.
4. Сохраните изменения в файле.

Конфигурационный файл будет создан.

Чтобы импортировать данные об активах:

1. Если вы хотите импортировать информацию об активе из MaxPatrol VM в Ядро Kaspersky SIEM Cloud без промежуточной проверки экспортированных данных, запустите утилиту kuma-ptvm со следующими параметрами:

   `kuma-ptvm --config <path to the kuma-ptvm-config.yaml file> --download --upload`

2. Если вы хотите проверить правильность данных, экспортированных из MaxPatrol VM, перед их импортом в Ядро Kaspersky SIEM Cloud:

   a. Запустите утилиту kuma-ptvm со следующими параметрами:

   `kuma-ptvm --config <path to the kuma-ptvm-config.yaml file> --download`

   Будет создан файл с именем в формате<tenant ID>.JSON. Также во время экспорта создается файл "tenants", содержащий список файлов JSON для загрузки в Ядро Kaspersky SIEM Cloud. Все файлы сохраняются в директории утилиты.

   b. Импортируйте информацию об активе в Ядро Kaspersky SIEM Cloud:

   `kuma-ptvm --config <path to the kuma-ptvm-config.yaml file> --upload`

   Чтобы просмотреть информацию о доступных командах утилиты, выполните команду --help.

   Информация об активе импортируется из MaxPatrol VM в Ядро Kaspersky SIEM Cloud. В консоли отображаются сведения о количестве новых и обновленных активов.

Возможные ошибки:

При запуске утилиты kuma-ptvm может вернуться ошибка `tls: failed to verify certificate: x509: certificate is valid for localhost`.

Чтобы решить проблему:

- Выпустите сертификат в соответствии с документацией MaxPatrol. Это рекомендованный способ решить эту ошибку.

- Выключите проверку сертификата.

  Чтобы выключить проверку сертификата, добавьте следующую строку в конфигурационный файл в разделе Параметры MaxPatrol:

  `ignore_server_cert: true`

В результате утилита запускается без ошибок.

Импорт данных об активах из MaxPatrol VM

В поставку Kaspersky SIEM Cloud входит утилита kuma-ptvm, которая состоит из исполняемого файла и файла конфигурации. Поддерживается работа под управлением ОС Windows и Linux. Утилита позволяет выполнить подключение к API MaxPatrol VM, получить данные об устройствах и их атрибутах, включая уязвимости, а также позволяет отредактировать данные об активах и импортировать данные с использованием API KUMA. Импорт данных поддерживается для версий MaxPatrol VM 1.1–2.7 включительно.

Настройка импорта информации об активах из MaxPatrol VM в Kaspersky SIEM Cloud состоит из следующих шагов:

1. Подготовительные действия в Kaspersky SIEM Cloud и MaxPatrol VM.

   Вам потребуется создать учетные записи пользователей и токен Kaspersky SIEM Cloud для операций через API.

2. Создание файла конфигурации с параметрами экспорта и импорта данных.

В зависимости от требуемого набора данных используйте один из файлов конфигурации:

- `kuma-ptvm-config.yaml` — для импорта информации об активах и уязвимостях.
- `kuma-ptvm-vulnerable-assets-config.yaml` — для импорта информации об активах и уязвимостях с возможностью дополнительной фильтрации.

Оба файла содержат обязательные и необязательные параметры. Заполните обязательные параметры и при необходимости укажите дополнительные параметры для фильтрации данных. В результате в Kaspersky SIEM Cloud будут импортированы только активы, соответствующие заданным параметрам.

Файл `kuma-ptvm-vulnerable-assets-config.yaml` дополнительно содержит секцию `Vulnerabilities assets settings`, в которой задаются параметры импорта информации об уязвимостях.

3. Экспорт данных из MaxPatrol VM и их импорт в Kaspersky SIEM Cloud с помощью утилиты kuma-ptvm.

   Запустите утилиту с соответствующим файлом конфигурации:

   - Для импорта информации об активах:

     ```
     ./kuma-ptvm --config <path to kuma-ptvm-config.yaml> --download --upload
     ```

   - Для импорта информации об активах и уязвимостях с возможностью дополнительной фильтрации:

     ```
     ./kuma-ptvm vulnerable-assets-api --config <path to kuma-ptvm-vulnerable-assets-config.yaml> --download --
     upload
     ```

   При выполнении команды данные сначала экспортируются из MaxPatrol VM и сохраняются в директории утилиты. Информация по каждому тенанту сохраняется в отдельный файл в формате JSON.

   При необходимости вы можете отредактировать полученные файлы. После этого данные из файлов импортируются в Kaspersky SIEM Cloud.

При повторном импорте уже существующие в Kaspersky SIEM Cloud активы будут перезаписаны. Таким образом устраненные уязвимости будут удалены.

Известные ограничения

Если для двух активов с разными FQDN указан один IP-адрес, Kaspersky SIEM Cloud импортирует такие активы как два разных актива, активы не будут объединены.

Если у актива два ПО с одинаковыми данными в полях name, version, vendor, Kaspersky SIEM Cloud импортирует эти данные как одно ПО, несмотря на разные пути установки ПО в активе.

Если в конфигурационном файле `kuma-ptvm-config.yaml` вы укажете параметр strict_import со значением false, то из MaxPatrol будут импортированы данные по всем активам, в том числе без обязательных для KUMA полей и с недопустимыми для KUMA значениями полей. Если FQDN актива содержит пробел или "_", данные по таким активам не будут импортированы в Kaspersky SIEM Cloud, в журнале будет указано, что такие активы пропущены при импорте.

Если при импорте происходит ошибка, информация об ошибке регистрируется в журнале и выполнение импорта прекращается.

Подготовительные действия

1. Создайте отдельную учетную запись пользователя в Kaspersky SIEM Cloud и в MaxPatrol VM с минимально необходимым набором прав на использование API-запросов.
2. Создайте учетные записи, для которых впоследствии сгенерируете API-токен.

   Требования к учетным записям, для которых генерируется API-токен:

   - Роль Главного администратора, Администратора тенанта, Аналитика второго уровня и Аналитика первого уровня.
   - Доступ к тенанту, в который будут импортированы активы.
   - В учетной записи пользователя в группе параметров **Права доступа через API** установлен флажок для POST /api/v3/assets/import.
3. Сгенерируйте токен для доступа к Kaspersky SIEM Cloud REST API.

Создание конфигурационного файла

Чтобы создать конфигурационный файл:

1. Перейдите в директорию установщика KUMA, выполнив следующую команду:

   ```
   cd kuma-ansible-installer/roles/kuma/files/
   ```

2. Распакуйте архив kuma-ptvm.tar.gz, выполнив следующую команду:

   `tar -xvf kuma-ptvm.tar.gz`

3. Скопируйте шаблон и создайте конфигурационный файл в зависимости от необходимого способа импорта активов.

   - Для стандартного импорта данных об активах:

     ```
     cp kuma-ptvm-config-template.yaml kuma-ptvm-config.yaml
     ```

   - Если необходимо дополнительно настроить параметры импорта данных об уязвимостях:

     ```
     cp kuma-ptvm-vulnerable-assets-config-template.yaml kuma-ptvm-vulnerable-assets-config.yaml
     ```

4. В зависимости от необходимого способа импорта активов отредактируйте параметры конфигурационного файла kuma-ptvm-config.yaml или параметры конфигурационного файла kuma-ptvm-vulnerable-assets-config-template.yaml.

5. Сохраните изменения в файле.

Конфигурационный файл будет создан. Теперь вы можете переходить к шагу Импорт информации об активах.

Импорт данных об активах

Чтобы импортировать информацию об активах из MaxPatrol VM в Kaspersky SIEM Cloud, используйте утилиту kuma-ptvm с конфигурационным файлом, созданным на предыдущем этапе.

Чтобы импортировать данные об активах:

1. Если вы хотите импортировать информацию об активах из MaxPatrol VM в Kaspersky SIEM Cloud без промежуточной проверки экспортированных данных, выполните команду download и upload одновременно. Выберите команду в зависимости от используемого конфигурационного файла:

   - Для `kuma-ptvm-config.yaml`:

     ```
     ./kuma-ptvm --config <path> --download --upload
     ```

   - Для `kuma-ptvm-vulnerable-assets-config.yaml`:

     ```
     kuma-ptvm vulnerable-assets-api --config <path> --download --upload
     ```

   где:

   <path> — полный путь к соответствующему конфигурационному файлу: `kuma-ptvm-config.yaml` или `kuma-ptvm-vulnerable-assets-config.yaml`.

2. Если вы хотите проверить правильность экспортированных из MaxPatrol VM данных перед импортом в Kaspersky SIEM Cloud, сначала выполните только экспорт:

   - Для `kuma-ptvm-config.yaml`:

     ```
     ./kuma-ptvm --config <path> --download
     ```

   - Для `kuma-ptvm-vulnerable-assets-config.yaml`:

     ```
     ./kuma-ptvm vulnerable-assets-api --config <path> --download
     ```

   где:

   <path> — полный путь к соответствующему конфигурационному файлу: `kuma-ptvm-config.yaml` или `kuma-ptvm-vulnerable-assets-config.yaml`.

При необходимости вы можете использовать параметр `--cvss-version <номер CVSS версии>`, чтобы указать, для какой версии CVSS нужно загрузить значения уязвимостей активов. Доступные значения:

- `2` – загружаются только значения CVSS версии 2.
- `3` – загружаются только значения CVSS версии 3. Если уязвимость описана только по версии 2, поле CVSS будет пустым.
- `latest` – загружаются значения последней доступной версии CVSS (значение по умолчанию). Если уязвимость не имеет значения CVSS версии 3, используется значение версии 2.

Примеры:

```
./kuma-ptvm vulnerable-assets-api --config <path> --cvss-version 2 --download
./kuma-ptvm vulnerable-assets-api --config <path> --cvss-version 3 --download
./kuma-ptvm vulnerable-assets-api --config <path> --cvss-version latest --download
```

где:

<path> — полный путь к соответствующему конфигурационному файлу: `kuma-ptvm-config.yaml` или `kuma-ptvm-vulnerable-assets-config.yaml`.

Утилита создаст отдельный JSON-файл для каждого тенанта, указанного в конфигурационном файле. Также будет создан файл tenants, содержащий список файлов, данные из которых будут импортированы в Kaspersky SIEM Cloud. Все файлы сохраняются в директории утилиты.

При необходимости проверьте и измените экспортированные данные:

- Распределите активы по соответствующим тенантам.
- Из файла тенанта по умолчанию default вручную перенесите данные активов в файлы нужных тенантов.
- В файле tenants отредактируйте список тенантов, активы которых будут импортированы в Kaspersky SIEM Cloud.

a. После проверки импортируйте информацию об активах в Kaspersky SIEM Cloud:

- Для `kuma-ptvm-config.yaml`:

  ```
  ./kuma-ptvm --config <path> --upload
  ```

- Для `kuma-ptvm-vulnerable-assets-config.yaml`:

  ```
  ./kuma-ptvm vulnerable-assets-api --config <path> --upload
  ```

где:

<path> — полный путь к соответствующему конфигурационному файлу: `kuma-ptvm-config.yaml` или `kuma-ptvm-vulnerable-assets-config.yaml`.

Чтобы просмотреть информацию о доступных командах утилиты, выполните команду `--help`.

Информация об активах будет импортирована из MaxPatrol VM в Kaspersky SIEM Cloud. В консоли отображаются сведения о количестве новых и обновленных активов.

Возможные ошибки

При запуске утилиты kuma-ptvm может вернуться ошибка `tls: failed to verify certificate: x509: certificate is valid for localhost`.

Решение:

- Выписать сертификат в соответствии с документацией MaxPatrol. Мы рекомендуем этот способ устранения ошибки, как предпочтительный.
- Отключить проверку сертификата.

  Чтобы отключить проверку сертификата, добавьте в конфигурационный файл в разделе `MaxPatrol settings` следующую строку:

  `ignore_server_cert: true`

В результате запуск утилиты выполняется без ошибок.

Параметры конфигурационного файла kuma-ptvm-vulnerable-assets-config-template.yaml

В таблице представлены параметры, доступные для настройки в файле `kuma-ptvm-vulnerable-assets-config-template.yaml`.

Описание параметров конфигурационного файла kuma-ptvm-vulnerable-assets-config-template.yaml

Параметр	Описание	Значения
Секция `General settings`		
`log_level`	Необязательный параметр. Уровень журналирования.	Доступные значения: • `trace` • `info` • `warning` • `error` Значение по умолчанию: `info`.
`strict_import`	Необязательный параметр. При экспорте активов из MaxPatrol проверять, заполнены ли обязательные для Kaspersky SIEM Cloud поля. Не экспортировать из MaxPatrol активы, не прошедшие проверку.	Доступные значения: • `true` – проверять наличие обязательных для Kaspersky SIEM Cloud полей. • `false` – не проверять наличие обязательных для Kaspersky SIEM Cloud полей. Значение по умолчанию: `false`. Мы рекомендуем указывать значение `true` при экспорте активов из MaxPatrol, это позволит выявить возможные ошибки в файлах JSON и исправить ошибки перед тем, как вы импортируете активы в Kaspersky SIEM Cloud.
Секция `KUMA settings`		
`endpoint`	Обязательный параметр. URL сервера Kaspersky SIEM Cloud API. Например: kuma.example.com:7223	–
`token`	Обязательный параметр. Токен Kaspersky SIEM Cloud API.	–
Секция `MaxPatrol settings`		
`endpoint`	Обязательный параметр. URL сервера MaxPatrol API.	–

Параметр	Описание	Значения
`token`	Необязательный параметр. Токен MaxPatrol API.	Для доступа к серверу MaxPatrol через API вам нужно указать значение параметра `token`.
Секция `Vulnerable Assets API Parameters` Ограничения: параметры `from` и `to` доступны в действующем контракте Swagger, но их поддержка зависит от развернутой у вас версии PTVM.		
`groups`	Необязательный параметр. Список идентификаторов групп активов, которые используются для фильтрации. В импорт будут включены только активы, относящиеся к указанным группам.	Пример: 4b7d711f-ae35-4c94-8625-4cfabf5fb99e
`statuses`	Необязательный параметр. Статус уязвимостей активов для фильтрации.	Доступные значения: • `new` — новая уязвимость. • `inProgress` — устранение уязвимости выполняется. • `awaitingFix` — ожидается устранение уязвимости. • `excluded` — уязвимость исключена из обработки. • `fixed` — уязвимость устранена. • `overdue` — срок устранения уязвимости истек. • `stale` — устаревшая уязвимость.
`severities`	Необязательный параметр. Степень критичности уязвимостей активов для фильтрации.	Доступные значения: • `none` — степень критичности не определена. • `low` — низкая. • `medium` — средняя. • `high` — высокая. • `critical` — критическая.
`from`	Необязательный параметр. Начальная дата и время периода фильтрации по дате последнего аудита актива включительно. Указывается в формате UTC.	Пример: 2026-02-10T00:58:00.123Z
`to`	Необязательный параметр. Конечная дата и время периода фильтрации по дате последнего аудита актива включительно. Указывается в формате UTC.	Пример: 2026-02-11T00:58:00.123Z
Секция `Vulnerability filter`		
`only_exploitable`	Необязательный параметр. Экспортировать из MaxPatrol только активы с уязвимостями, для которых известны эксплойты.	Доступные значения: • `true` – экспортировать только активы с уязвимостями, для которых известны эксплойты. • `false` – экспортировать все активы. Значение по умолчанию: `false`.
Секция `Tenant map`		
`id`	Обязательный параметр. Идентификатор тенанта в Kaspersky SIEM Cloud. Активы распределяются по тенантам в том порядке, в каком тенанты указаны в конфигурационном файле: чем выше тенант в списке, тем выше у него приоритет. Таким образом вы можете указывать и перекрывающиеся подсети.	–
`fqdn`	Необязательный параметр. Регулярное выражение для поиска FQDN актива.	–
`networks`	Необязательный параметр. Одна или несколько подсетей.	–
`default_tenant`	Необязательный параметр. Идентификатор тенанта Kaspersky SIEM Cloud по умолчанию, куда будут поступать данные об активах, которые не удалось распределить по тенантам, заданным в секции параметров Tenants.	–

Импорт информации об активах из KICS for Networks

Вы можете импортировать информацию об активах, защищаемых KICS for Networks, в Kaspersky SIEM Cloud. Для этого вам требуется предварительно настроить интеграцию между приложениями.

После создания интеграции с KICS for Networks задачи на получение данных об активах KICS for Networks создаются автоматически. Это происходит в следующих случаях:

- Сразу после создания новой интеграции.
- Сразу после изменения параметров существующей интеграции.
- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 12 часов. Расписание можно изменить.

Задачи на обновление данных об учетных записях можно создать вручную.

Чтобы настроить задачу на обновление данных об активах KICS for Networks для тенанта:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Выберите тенант, для которого вы хотите импортировать активы KICS/KATA.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** в разделе **Обнаружение и реагирование** нажмите **Параметры активов**.
4. Убедитесь, что на вкладке **Импорт KICS/KATA** включен переключатель **Состояние**.
5. Настройте импорт данных актива:
   - Чтобы настроить периодический импорт данных, в поле **Интервал импорта (в часах)** укажите интервал, через который OSMP Console будет обновлять данные об активах KICS/KATA.
   - Чтобы запустить импорт вручную, нажмите на кнопку **Импорт**.

В OSMP Console в разделе Диспетчер задач будет добавлена **задача** на получение данных об учетных записях выбранного тенанта.

Примеры сравнения полей активов при импорте

Каждый импортируемый актив сравнивается с активом OSMP.

Проверка на совпадение значений в полях IP, MAC, FQDN по двум полям

Сравниваемые активы	Сравниваемые поля		
	FQDN	IP	MAC
Актив KUMA	Есть	Есть	Не заполнено
Импортируемый актив 1	Есть, совпадает	Есть, совпадает	Есть
Импортируемый актив 2	Есть, совпадает	Есть, совпадает	Не заполнено
Импортируемый актив 3	Есть, совпадает	Не заполнено	Есть
Импортируемый актив 4	Не заполнено	Есть, совпадает	Есть
Импортируемый актив 5	Есть, совпадает	Не заполнено	Не заполнено
Импортируемый актив 6	Не заполнено	Не заполнено	Есть

Результаты сравнения:

- Импортируемый актив 1 и актив OSMP: для обоих активов заполнены и совпадают поля FQDN и IP, по полю MAC нет противоречия. Активы объединены.
- Импортируемый актив 2 и актив OSMP: для обоих активов заполнены и совпадают поля FQDN и IP. Активы объединены.
- Импортируемый актив 3 и актив OSMP: для обоих активов заполнены и совпадают поля FQDN и MAC, по полю IP нет противоречия. Активы объединены.
- Импортируемый актив 4 и актив OSMP: для обоих активов заполнено и совпадает поле IP, по полям FQDN и MAC нет противоречия. Активы объединены.
- Импортируемый актив 5 и актив OSMP: для обоих активов заполнено и совпадает поле FQDN, по полям IP и MAC нет противоречия. Активы объединены.
- Импортируемый актив 6 и актив OSMP: для активов нет ни одного совпадающего поля. Активы не объединяются.

Проверка на совпадение значений в полях IP, MAC, FQDN по одному полю

Сравниваемые активы	Сравниваемые поля		
	FQDN	IP	MAC
Актив OSMP	Не заполнено	Есть	Не заполнено
Импортируемый актив 1	Есть	Есть, совпадает	Есть
Импортируемый актив 2	Есть	Есть, совпадает	Не заполнено
Импортируемый актив 3	Есть	Не заполнено	Есть
Импортируемый актив 4	Не заполнено	Не заполнено	Есть

Результаты сравнения:

- Импортируемый актив 1 и актив OSMP: для обоих активов заполнено и совпадает поле IP, по полям FQDN и MAC нет противоречия. Активы объединены.
- Импортируемый актив 2 и актив OSMP: для обоих активов заполнено и совпадает поле IP, по полям FQDN и MAC нет противоречия. Активы объединены.
- Импортируемый актив 3 и актив OSMP: для активов нет ни одного совпадающего поля. Активы не объединяются.
- Импортируемый актив 4 и актив OSMP: для активов нет ни одного совпадающего поля. Активы не объединяются.

Назначение активу категории

Назначение категории одному активу в свойствах актива

Этот способ не подходит для назначения категории активам KSC и KICS. Следуйте инструкции по назначению категории одному или нескольким активам.

Чтобы назначить категорию одному активу:

1. В главном меню перейдите в раздел **Управление активами → Управляемые устройства → Обнаружение и реагирование**.
2. Нажмите на кнопку **Показать навигацию** и выберите тенант и категорию с требуемыми активами.

   Отобразится таблица активов.
3. Выберите актив и в открывшемся меню выберите **Подробнее**.
4. В открывшемся окне нажмите на кнопку **Изменить**.
5. На вкладке **Дополнительно** в поле **Категории** выберите категорию.

   Если вы хотите перенести актив в раздел **Активы без категории**, вам требуется удалить существующие для актива категории, нажав на кнопку ×.
6. Нажмите на кнопку **Сохранить**.

Категория будет назначена.

Назначение категории одному или нескольким активам

Чтобы назначить категорию одному или нескольким активам:

1. В главном меню перейдите в раздел **Управление активами** → **Управляемые устройства** → **Обнаружение и реагирование**.
2. Нажмите на кнопку **Показать навигацию** и выберите тенант и категорию с требуемыми активами.

   Отобразится таблица активов.
3. Установите флажки рядом с активами, для которых вы хотите изменить категорию.
4. Нажмите на кнопку **Привязать к категории**.
5. В открывшемся окне выберите категорию.
6. Нажмите на кнопку **Привязать**.

Категория будет назначена.

Не назначайте активам категорию `Categorized assets`.

Привязка группы активов к категории

Чтобы привязать группу активов к категории:

1. В разделе **Управление активами** → **Управляемые устройства** → **Обнаружение и реагирование** в заголовке таблицы со списком активов установите флажок.
2. Выделите все активы, видимые на странице или все активы, согласно условию выбора.

   Кнопка **Привязать к категории** становится активной и открывает доступные категории.
3. Нажмите на кнопку **Привязать к категории** и выберите одну или несколько категорий для привязки.
4. Нажмите **OK**.

   Активы привязываются к выбранным категориям или папке.

Отвязка группы активов от категории

Чтобы отвязать группу активов от категории:

1. Выберите одну категорию (тенант) в навигационной панели.

   Отображается список активов категории.

   В свойства папки добавится кнопка **Очистить категорию**.

2. В контекстном меню категории выберите **Очистить категорию**.

   Появляется диалоговое окно с запросом подтверждения и числом отвязываемых активов.

   Эта опция позволяет отвязывать все активы в выбранной категории, не только видимые на странице. Активы в дочерних категориях не отвязываются.

3. В диалоговом окне нажмите **OK**.

   Все выбранные активы будут отвязаны от выбранной категории.

Изменение параметров активов

В OSMP можно изменять параметры активов. У добавленных вручную активов можно изменять все параметры. У активов, импортированных из Kaspersky Security Center, можно изменить только название актива и его категорию.

Чтобы изменить параметры актива:

1. В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства → Обнаружение и реагирование**.

2. Выберите категорию с требуемыми активами.

   Отобразится таблица активов.

3. Выберите актив и нажмите **Подробнее**.

4. В открывшемся окне нажмите на кнопку **Изменить**.

   Откроется окно **Изменить актив**.

5. Внесите необходимые изменения в доступные поля:

   - **Имя актива** (обязательно). Это единственное поле, доступное для редактирования у активов, импортированных из Kaspersky Security Center или KICS for Networks.
   - **IP-адрес** и/или **FQDN** (обязательно). Вы можете указать несколько FQDN через запятую.
   - **MAC-адрес.**
   - **Владелец.**
   - **Информация о программном обеспечении**:
     - **Название ОС**
     - **Сборка ОС**
   - **Информация об оборудовании**:

     Параметры оборудования

     В раздел **Информация об оборудовании** можно добавить сведения об оборудовании актива:

Доступные поля для описания CPU актива:

- **Название процессора**
- **Частота процессора**
- **Количество ядер процессора**

  Активу можно добавить процессоры с помощью ссылки **Добавить процессор**.

Доступные поля для описания диска актива:

- **Свободных байт на диске**
- **Объем диска**

  Активу можно добавить диски с помощью ссылки **Добавить диск**.

Доступные поля для описания RAM актива:

- **Частота оперативной памяти**
- **Общий объем ОЗУ**

Доступные поля для описания сетевой карты актива:

- **Название сетевой карты**
- **Производитель сетевой карты**
- **Версия драйвера сетевой карты**

  Активу можно добавить сетевые карты с помощью ссылки **Добавить сетевую карту**.

6. На вкладке **Дополнительно** в поле **Категории** выберите категорию.

> Также можно выбрать актив и перетащить его в нужную категорию. Эта категория будет добавлена в список категорий актива.

> Не назначайте активам категорию `Categorized assets`.

7. Нажмите на кнопку **Сохранить**.

Параметры актива изменены.

Архивирование активов

В OSMP Console функция архивирования доступна для следующих типов активов:

- Для активов, импортированных из Kaspersky Security Center и KICS.

  Если OSMP Console не получила информацию об активе в момент импорта, актив автоматически переводится в состояние архивного и хранится в базе данных в течение срока, который вы можете задать в параметре **Срок хранения архивных активов**. Значение по умолчанию – 0 дней. Это означает, что архивные активы хранятся бессрочно Архивный актив станет активным, если OSMP получит информацию об активе от источника до истечения срока хранения архивных активов.

- Для объединенных активов.

  При импорте OSMP Console выполняет проверку на уникальность среди активов, импортированных из Kaspersky Security Center и KICS, и активов, добавленных вручную. Если поля импортированного актива и добавленного вручную актива совпадают, активы объединяются в один актив, который считается импортированным и может стать архивным.

- Активы, добавленные вручную в консоли или с помощью API, архивируются и хранятся в базе данных в течение периода, указанного в параметре **Срок хранения архивных активов (в днях)**. Значение по умолчанию – 0 дней. Это означает, что архивные активы хранятся бессрочно Вы можете использовать параметр **Разархивировать активы**, если хотите сделать актив действующим до истечения срока хранения архивных активов.

Актив становится архивным при следующих условиях:

- Вы используете параметр **Архивировать активы** для активов, созданных вручную в консоли или с помощью API.
- OSMP Console не получила информацию об активе от Kaspersky Security Center или KICS for Networks.
- Отключена интеграция с Kaspersky Security Center.

  Если вы отключили интеграцию с Kaspersky Security Center, в течение 30 дней актив будет считаться активным. По истечении 30 дней актив автоматически переводится в состояние архивного и хранится в базе данных в течение времени, указанного в параметре **Срок хранения архивных активов (в днях)**.

Обновление актива не происходит в следующих случаях:

- Данные об активе Kaspersky Security Center не обновлялись больше срока хранения архивных активов.
- Данные об активе отсутствуют в Kaspersky Security Center или KICS for Networks.
- Соединение с Сервером администрирования Kaspersky Security Center отсутствует больше 30 дней.

Чтобы изменить статус архива для актива или группы активов, созданных вручную:

1. В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства → Обнаружение и реагирование**.

   Откроется таблица активов.

2. В таблице активов установите флажки рядом с активами, созданными вручную, для которых вы хотите изменить статус архивирования.

3. На панели инструментов в верхней части таблицы ресурсов нажмите на одну из следующих кнопок:

   - **Архивировать активы**, чтобы поместить выбранные активы в архив.
   - **Разархивировать активы**, чтобы восстановить выбранные архивные активы.

   Архивный статус актива изменен. Вы можете отфильтровать активы по их архивному статусу в таблице активов в раскрывающемся списке столбца **Отправлено в архив**, выбрав один из вариантов: **Да**, чтобы отображать только архивные активы, или **Нет**, чтобы отображать только действующие активы.

Чтобы настроить срок хранения архивных активов:

1. В главном окне приложения перейдите в раздел **Параметры → Тенанты**.
2. Выберите тенант, для которого вы хотите изменить период хранения архивных активов.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** в разделе **Обнаружение и реагирование** нажмите **Параметры активов**.
4. На вкладке **Общие** введите новое значение в поле **Срок хранения архивных активов (в днях)**.

   Значение по умолчанию – 30 дней. Введите значение 0, чтобы хранить архивные активы бессрочно.
5. Нажмите на кнопку **Сохранить и закрыть**.

   Срок хранения архивных активов будет настроен.

Информация об архивном активе остается доступной для просмотра в карточке алертов и инцидентов.

Чтобы просмотреть карточку архивного актива:

1. В главном меню перейдите в раздел **Мониторинг**, выберите раздел **Алерты** или **Инциденты**.

   Отобразится список алертов или инцидентов.
2. Откройте карточку алерта или инцидента, связанного с архивным активом.

   Вам будет доступен просмотр информации в карточке архивного актива.

Удаление активов

Вы можете удалять активы в разделе **Управление активами → Активы (Устройства) → Администрирование и защита**. На вкладке **Обнаружение и реагирование** OSMP Console удаляет только архивные активы только автоматически. Удалить активы вручную невозможно. OSMP Console удалит архивный актив, если информация об активе не обновлялась больше срока хранения архивных активов.

Удаление категории активов

Удаление категории выполняется в два этапа: перемещение в архив и безвозвратное удаление. Архивирование позволяет проверить, ссылаются ли на категорию какие-либо ресурсы, прежде чем она будет окончательно удалена из системы.

Если категория архивируется в родительском экземпляре OSMP Console, соответствующая категория во всех дочерних экземплярах OSMP Console также архивируется. Затем система проверяет, ссылаются ли все еще какие-либо ресурсы на заархивированную категорию. Если не осталось ссылок, категория будет удалена безвозвратно.

Чтобы удалить категорию активов:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства** → **Обнаружение и реагирование**.
2. В дереве категорий нажмите на значок (⋮) рядом с категорией, которую вы хотите удалить.
3. В контекстном меню нажмите **Архив**.
4. В диалоговом окне **Удалить категорию?** нажмите на кнопку **OK** для подтверждения.

Если ресурсы все еще привязаны к категории, категория остается в архиве до тех пор, пока не будут удалены все связи.

Заархивированные категории не отображаются в списке категорий, но могут оставаться доступными в фильтрах, которые ссылаются на категорию. Свойства категории остаются доступными для просмотра, а связи ресурсов можно удалить. Изменение параметров категории невозможно, кроме названия категории.

Дополнительные ограничения применяются к категориям, содержащим дочерние категории:

- Родительская категория не может быть перемещена в архив или удалена, если в ней есть хотя бы одна дочерняя категория, не перемещенная в архив.
- Перед удалением родительской категории все дочерние категории должны быть заархивированы или удалены без возможности восстановления.
- После того как все дочерние категории перемещены в архив, родительская категория следует стандартному процессу перемещения в архив и удаления.

Категория удаляется безвозвратно только если все ссылки на категорию удалены и все ограничения иерархии выполнены.

Массовое удаление активов

В веб-консоли вы можете осуществить множественный выбор активов с помощью фильтра и удалить все выбранные активы.

Для удаления активов у вас должны быть права на удаление активов.

Массовое удаление активов

Чтобы удалить все выбранные активы:

1. В веб-консоли перейдите в раздел **Управление активами** → **Управляемые устройства** → **Администрирование и защита** и выберите категорию с требуемыми активами.

   Отобразится таблица со списком активов.

2. В шапке таблицы со списком активов установите флажок.

   Вам будет предложено два варианта удаления: все активы или все активы, видимые на странице.

3. Нажмите на **Выбрать все на странице** или **Выбрать все**.

   Кнопка **Удалить** станет активной.

4. Нажмите на кнопку **Удалить**.

   Появится окно с запросом подтверждения удаления и с информацией о том, что удаленные активы не будут доступны в алертах, инцидентах и виджетах.

   Внизу страницы отобразится количество выбранных для удаления активов.

5. Нажмите **ОК**.

   Если вы нажали на **Выбрать все**, то перед подтверждением удаления нужно ввести запрашиваемую сгенерированную строку в текстовое поле окна.

Все выбранные активы будут удалены.

Удаление папок с активами

Для удаления папки вы можете или отвязать (при этом активы будут отвязаны, но не удалены) все активы от папки и затем удалить саму папку, или удалить все активы (активы будут удалены из программы), а затем удалить папку.

Обновление приложений сторонних производителей и закрытие уязвимостей на активах Kaspersky Security Center

Вы можете обновлять приложения сторонних производителей, в том числе приложения Microsoft, установленные на активах Kaspersky Security Center, и закрывать уязвимости этих приложений.

Предварительно вам нужно создать задачу *Установка требуемых обновлений и закрытие уязвимостей* на выбранном сервере Администрирования Kaspersky Security Center со следующими параметрами:

- Приложение – Kaspersky Security Center.
- Тип задачи – *Установка требуемых обновлений и закрытие уязвимостей*.
- Устройства, которым будет назначена задача – вам требуется назначить задачу корневой группе администрирования.

- Правила для установки обновлений:
  - Устанавливать только утвержденные обновления.
  - Закрывать уязвимости с уровнем критичности равным или выше (необязательный параметр).

    Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (*Средний*, *Высокий* или *Предельный*). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.
- Запуск по расписанию – расписание, в соответствии с которым выполняется задача.

О способах создания задачи см. подробнее в *справке Kaspersky Security Center*.

Задача *Установка требуемых обновлений и закрытие уязвимостей* доступна при наличии лицензии на Системное администрирование.

Далее вам требуется установить обновления для приложений сторонних производителей и закрыть уязвимости на активах в OSMP.

Чтобы установить обновления и закрыть уязвимости приложений сторонних производителей на активе в OSMP:

1. Откройте окно информации об активе одним из следующих способов:
   - В главном окне приложения перейдите в раздел **Управление активами → Управляемые устройства → Обнаружение и реагирование**, выберите категорию с соответствующими активами, затем выберите актив и нажмите **Подробнее**.
   - В главном окне приложения перейдите в раздел **Мониторинг → Поиск угроз**. Выполните поиск и фильтрацию событий. Затем выберите требуемое событие и перейдите по ссылке в одном из следующих полей: SourceAssetID, DestinationAssetID или DeviceAssetID.
2. В окне информации об активе раскройте список **Уязвимости Kaspersky Security Center**.
3. Установите флажки рядом с приложениями, которые вы хотите обновить.
4. Нажмите на ссылку **Загрузить обновления**.
5. В открывшемся окне установите флажок рядом с идентификатором уязвимости, которую вы хотите закрыть.
6. Если в столбце **Лицензионное соглашение принято** для выбранного идентификатора отображается **Нет**, нажмите на кнопку **Принять обновления**.
7. Перейдите по ссылке в столбце **URL Лицензионного соглашения** и ознакомьтесь с текстом Лицензионного соглашения.
8. Если вы с ним согласны, нажмите **Принять Лицензионные соглашения**.

   Напротив идентификатора уязвимости, для которого было принято Лицензионное соглашение, в столбце **Лицензионные соглашения приняты** отобразится **Да**.

9. Повторите шаги 7–10 для каждого требуемого идентификатора уязвимости.

10. Нажмите на кнопку **OK**.

Обновления будут загружены и установлены на активы, того сервера Администрирования, где была запущена задача, а также на активы всех подчиненные серверы Администрирования.

> Условия Лицензионного соглашения для обновления и закрытия уязвимостей требуется принять на каждом подчиненном сервере Администрирования отдельно.

Обновления устанавливаются на активы, на которых была обнаружена уязвимость.

Вы можете обновить список уязвимостей для актива в окне информации об активе, нажав на ссылку **Обновить**.

Перемещение активов в выбранную группу администрирования

Вы можете перемещать активы в выбранную группу администрирования Kaspersky Security Center. В этом случае на активы будут распространятся групповые политики и задачи. Подробнее о политиках и задачах Kaspersky Security Center см. *справку Kaspersky Security Center*.

Группы администрирования добавляются в OSMP Console при загрузке иерархии во время импорта активов из Kaspersky Security Center. Предварительно вам требуется настроить интеграцию OSMP Console с Kaspersky Security Center.

Чтобы переместить один актив в выбранную группу администрирования:

1. Откройте окно информации об активе одним из следующих способов:

   - В веб-консоли перейдите в раздел **Управление активами** → **Управляемые устройства** → **Обнаружение и реагирование**, выберите категорию с соответствующими активами, затем выберите актив и нажмите **Подробнее**.

   - В веб-консоли перейдите в раздел **Мониторинг** → **Алерты**, перейдите по ссылке с соответствующим алертом, затем в разделе **Активы** выберите актив и нажмите на кнопку **Просмотреть свойства**.

2. В окне информации об активе нажмите **Реагирование** → **Переместить в группу**.

3. В открывшемся окне выберите группу.

   > Выбранная группа должна принадлежать тому же тенанту, которому принадлежит актив.

4. Нажмите на кнопку **Сохранить**.

Выбранный актив будет перемещен.

Чтобы переместить несколько активов в выбранную группу администрирования:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства** → **Обнаружение и реагирование**.
2. Выберите категорию с требуемыми активами.
3. Установите флажки рядом с активами, которые хотите переместить в группу.
4. Нажмите **Реагирование** → **Переместить в группу**.

   Кнопка активна, если все выбранные активы принадлежат одному серверу Администрирования.

5. В открывшемся окне выберите группу.
6. Нажмите на кнопку **Сохранить**.

Выбранные активы будут перемещены.

Вы можете посмотреть, к какой группе принадлежит актив, в информации об активе.

Сведения об активах Kaspersky Security Center обновляются в OSMP Console в момент импорта информации об активах из Kaspersky Security Center. Это означает, что может возникнуть ситуация, когда в Kaspersky Security Center активы были перемещены между группами администрирования, однако в OSMP Console эти сведения еще не отображаются. При попытке переместить такой актив в группу администрирования, в которой он уже находится, OSMP Console возвращает ошибку **Не удалось переместить активы в другую группу KSC**.

Аудит активов

В Kaspersky SIEM Cloud можно настроить создание событий аудита активов при следующих условиях:

- Актив добавлен в Kaspersky SIEM Cloud. Отслеживается создание актива вручную, а также создание при импорте через REST API, импорте из Kaspersky Security Center или KICS for Networks.
- Параметры актива изменены. Отслеживается изменение значение следующих полей актива:
  - Имя;
  - IP-адрес;
  - MAC-адрес;
  - FQDN;
  - Операционная система.

  Изменения полей может происходить при обновлении актива во время импорта.

- Актив удален из Kaspersky SIEM Cloud. Отслеживается удаление активов вручную, а также автоматическое удаление активов, импортированных из Kaspersky Security Center и KICS for Networks, данные о которых перестали поступать.

- Сведения об уязвимости добавлены в актив. Отслеживается появление у активов новых данных об уязвимостях. Сведения об уязвимостях могут быть добавлены в актив, например, при импорте активов из Kaspersky Security Center или KICS for Networks.

- Уязвимость актива закрыта. Отслеживается удаление из актива сведений об уязвимости. Уязвимость считается закрытой, если данные о ней перестают поступать из всех источников, из которых ранее были получены сведения о ее появлении.

- Актив добавлен в категорию. Отслеживается присвоении активу категории активов.

- Актив удален из категории. Отслеживается удаление актива из категории активов.

По умолчанию, если аудит активов включен, при описанных выше условиях Kaspersky SIEM Cloud создает не только события аудита (`Type = 4`), но и базовые события (`Type = 1`).

События аудита активов можно отправлять, например, на хранение или в коррелляторы.

Настройка аудита активов

Чтобы настроить аудит активов:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.

2. Выберите тенант, для которого вы хотите настроить аудит активов.

   Откроется окно свойств тенанта.

   Если вы хотите настроить аудит активов для нового тенанта, сначала создайте его.

3. На вкладке **Параметры** в разделе **Обнаружение и реагирование** нажмите **Аудит активов**.

4. Выберите для каждого условия создания событий аудита активов, куда будут отправляться создаваемые события:

   a. В блоке параметров нужного типа событий аудита активов в раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, куда следует отправлять создаваемые события:

      - Выберите **Хранилище**, если хотите, чтобы события отправлялись в хранилище.

      - Выберите **Коррелятор**, если хотите, чтобы события отправлялись в коррелятор.

      - Выберите **Другое**, если хотите выбрать иную точку назначения.

        К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях приложения.

   Откроется окно **Добавить точку назначения**, где вам требуется параметры пересылки событий.

b. В раскрывающемся списке **Точка назначения** выберите существующую точку назначения или выберите пункт **Создать**, если хотите создать точку назначения.

При создании новой точки назначения заполните параметры, как указано в описании точки назначения.

c. Нажмите на кнопку **Сохранить**.

Точка назначения добавлена к условию создания событий аудита активов. Для каждого условия можно добавить несколько точек назначения.

5. Нажмите на кнопку **Сохранить**.

Аудит активов настроен. События аудита активов будут создаваться для тех условий, для которых были добавлены точки назначения. Нажмите на кнопку **Сохранить**.

Хранение и поиск событий аудита активов

События аудита активов считаются базовыми и не заменяют собой событий аудита. События аудита активов можно искать по следующим параметрам:

Поле события	Значение
DeviceVendor	`"Лаборатория Касперского".`
DeviceProduct	`KUMA`
DeviceEventCategory	`Audit assets`

Включение и выключение аудита активов

Вы можете включить или выключить аудит активов для тенанта.

Чтобы включить или выключить аудит активов для тенанта:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Выберите тенант, для которого вы хотите включить или выключить аудит активов.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** в разделе **Обнаружение и реагирование** нажмите **Аудит активов**.
4. Включите или выключите переключатель **Сбор событий аудита**.
5. Нажмите на кнопку **Сохранить**.

По умолчанию при включенном аудите активов при возникновении условия аудита одновременно создаются два типа событий: базовое событие и событие аудита.

Вы можете отключить создание базовых событий одновременно с событиями аудита.

Чтобы включить или выключить для отдельного условия создание базовых событий:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты**.
2. Выберите тенант, для которого вы хотите включить или выключить условие для генерации событий аудита активов.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** в разделе **Обнаружение и реагирование** нажмите **Аудит активов**.
4. Нажмите имя действия с условием, чтобы включить или выключить создание соответствующих базовых событий.
5. Нажмите на кнопку **Сохранить**.

Если условие выключено, создаются только события аудита, базовые события создаваться не будут.

Настраиваемые поля активов

В дополнение к существующим полям модели данных актива можно создать настраиваемые поля активов. Данные из настраиваемых полей активов отображаются при просмотре информации об активе. Данные в настраиваемые поля можно записывать вручную или через API.

Вы можете создать или изменить настраиваемые поля.

Чтобы создать настраиваемое поле активов:

1. В веб-консоли перейдите в раздел **Параметры** → **Тенанты**.
2. Выберите тенант, для которого вы хотите изменить период хранения архивных активов.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** в разделе **Обнаружение и реагирование** нажмите **Параметры активов**.
4. На вкладке **Общая** в поле **Пользовательские поля** нажмите на кнопку **Добавить**.

   В таблице **Пользовательские поля** добавится пустая строка. Вы можете добавить сразу несколько строк с параметрами настраиваемого поля.
5. Заполните столбцы с параметрами настраиваемого поля:

   - **Название** (обязательно) – от 1 до 128 символов в кодировке Unicode.
   - **Значение по умолчанию** – от 1 до 1024 символов в кодировке Unicode.
   - **Маска** – от 1 до 1024 символов в кодировке Unicode.
6. Нажмите на кнопку **Сохранить**.

К модели данных активов добавлено настраиваемое поле.

Чтобы удалить или изменить настраиваемое поле активов:

1. В веб-консоли перейдите в раздел **Параметры** → **Тенанты**.
2. Выберите тенант, для которого вы хотите изменить период хранения архивных активов.

   Откроется окно свойств тенанта.
3. На вкладке **Параметры** в разделе **Обнаружение и реагирование** нажмите **Параметры активов**.
4. На вкладке **Общие** внесите необходимые изменения в таблицу **Пользовательские поля**:
   - Чтобы удалить настраиваемое поле, установите флажок рядом с нужным полем и нажмите на кнопку **Удалить**. При удалении поля также удаляются записанные в это поле данные для всех активов.
   - Вы можете изменить значения параметров полей. При изменении значения по умолчанию уже записанные в поля активов данные не меняются.
   - Чтобы изменить порядок отображения полей, используйте кнопки **Поднять** и **Опустить**.
5. Нажмите на кнопку **Сохранить**.

Изменения внесены.

Реагирование

Правила реагирования запускают для заданных событий автоматический запуск пользовательского скрипта.

Вы можете настроить правила реагирования в разделе **Мониторинг** → **Ресурсы и сервисы** → **Правила реагирования**, а затем выбрать созданное правило реагирования в раскрывающемся списке в настройках коррелятора. Правила реагирования также можно настроить напрямую в настройках коррелятора.

Правила реагирования для пользовательского скрипта

Вы можете создать скрипт с командами, которые требуется выполнить на сервере Kaspersky SIEM Cloud при обнаружении выбранных событий, и настроить правила реагирования для автоматического запуска этого скрипта. В этом случае решение запустит скрипт при получении событий, соответствующих правилам реагирования.

Файл скрипта хранится на сервере, где установлен сервис коррелятора, использующий ресурс реагирования: `/opt/kaspersky/kuma/correlator/<correlator_ID>/scripts`. Пользователю `kuma` этого сервера требуются права на запуск скрипта.

При создании и изменении правил реагирования для произвольного скрипта вам требуется задать значения для следующих параметров.

Вкладка Общие

Вкладка Общие

Параметр	Описание
Название	Обязательный параметр. Уникальное имя ресурса. Должно содержать от 1 до 128 символов в кодировке Unicode.
Тенант	Обязательный параметр. Название тенанта, которому принадлежит ресурс.
Тип	Обязательный параметр. Тип правила реагирования, **Запуск скрипта**.
Время ожидания	Количество секунд, в течение которого должно завершиться выполнение скрипта. Если это время превышено, выполнение скрипта прерывается.
Название скрипта	Обязательный параметр. Имя файла скрипта. Если ресурс реагирования прикреплен к сервису коррелятора, но в папке `/opt/kaspersky/kuma/correlator/<correlator_ID>/scripts` файл скрипта отсутствует, коррелятор не будет работать.
Аргументы скрипта	Параметры или значения полей событий, которые необходимо передать скрипту. Если в скрипте производятся какие-либо действия с файлами, к ним следует указывать абсолютный путь. Параметры можно обрамлять кавычками ("). Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это имя поля события, значение которого должно быть передано в скрипт. Пример: `-n "\"usr\": {{.SourceUserName}}"`
Обработчики	Количество обработчиков, которые сервис может запускать одновременно для параллельной обработки правил реагирования. По умолчанию количество обработчиков соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.
Описание	Описание ресурса. Вы можете добавить до 4000 символов в кодировке Unicode.

Фильтр

Используется для определения условий, при соответствии которым события будут обрабатываться с применением правила реагирования. В раскрывающемся списке можно выбрать существующий фильтр или **Создать** новый фильтр.

Создание фильтра в ресурсах

Все поля события Kaspersky SIEM Cloud имеют значение по умолчанию. Для всех числовых полей это значение равно `0`. Для всех строковых полей значение по умолчанию – пустая строка. Если событие не имеет какого-то поля, это значит, что полю присвоено значение по умолчанию. Поэтому фильтр может сработать на событие, даже если у этого события нет указанного в фильтре поля. Например, если вы в фильтре указали условие `DestinationPort <= 1024`, но событие не содержит поля `DestinationPort`, фильтр сработает, так как по умолчанию `DestinationPort = 0`.

Чтобы создать фильтр:

1. В раскрывающемся списке **Фильтр** выберите **Создать**.
2. Если вы хотите сохранить фильтр и использовать его в качестве фильтра для других ресурсов, установите флажок **Сохранить фильтр**. По умолчанию флажок снят.
3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название нового фильтра. Максимальная длина названия: до 128 символов в кодировке Unicode.
4. Выберите режим создания фильтра: **Конструктор** или **Код**.

   При формировании условий фильтрации вы можете переключаться между режимами. При переключении между режимами сформированные условия фильтров сохраняются. Если после привязки созданного фильтра к ресурсу на вкладке **Код** не отображается код фильтра, выберите вкладку **Конструктор**, после чего снова выберите вкладку **Код** для отображения кода фильтра.
5. Если вы выбрали вариант **Конструктор**, выполните следующие действия:

   a. В раскрывающемся списке выберите логический оператор:

   - **И** – отбирает события, которые соответствуют всем указанным условиям.
   - **ИЛИ** – отбирает события, которые соответствуют одному из указанных условий.
   - **НЕ** – отбирает события, которые не соответствуют всем указанным условиям.

   b. Нажмите на кнопку **Добавить условие**.

   c. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.

   d. В последовательно отображающихся раскрывающихся списках выберите операнды и операторы фильтра.

   Операнды фильтров

   - **Поля событий** – поле события, которое требуется использовать как операнд фильтра.
   - **Активные листы** – активный лист или поле активного листа, которое требуется использовать как операнд фильтра. При выборе активного листа укажите одно или несколько полей событий, которые используются для создания записи активного листа и выступают ключом записи активного листа. Для завершения указания полей событий нажмите комбинацию клавиш **Ctrl**/**Command**+**F1**.

     Если вы не указали оператор **inActiveList**, вам нужно указать имя поля активного листа, которое требуется использовать как операнд фильтра.
   - **Словари** – значение из ресурса словарь, которое требуется присвоить операнду. Дополнительные параметры:
     - **словарь** (обязательно) – словарь, который требуется использовать.
     - **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.
   - **Контекстные таблицы** – в этом разделе вы можете указать значение контекстной таблицы, которое требуется использовать как операнд фильтра. При выборе контекстной таблицы вам нужно указать поле события.
     - **название контекстной таблицы** (обязательно) – контекстная таблица, которую требуется использовать.
     - **ключевые поля** (обязательно) – поля событий или локальные переменные, которые используются для создания записи контекстной таблицы и выступают ключом записи контекстной таблицы.
     - **поле** – имя поля контекстной таблицы, из которого требуется извлечь значение операнда.
     - **индекс** – индекс списочного поля таблицы, из которого требуется извлечь значение операнда.
   - **Таблицы** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
     - **словарь** (обязательно) – тип словаря. Вам нужно выбрать тип словаря **Таблица**.
     - **ключевые поля** (обязательно) – поля событий, которые используются для формирования ключа значения словаря.
   - **TI** – параметры чтения данных Kaspersky CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
     - **поток** (обязательно) – категория угрозы Kaspersky CyberTrace.
     - **ключевые поля** (обязательно) – поле события с индикаторами угроз Kaspersky CyberTrace.
     - **поле** (обязательно) – поле фида Kaspersky CyberTrace с индикаторами угроз.

- **Константа** – пользовательское значение, которое требуется присвоить операнду. Дополнительные параметры:
  - **значение** (обязательно) – константа, которую требуется присвоить операнду.
- **Список** – пользовательские значения, которые требуется присвоить операнду. Дополнительные параметры:
  - **значение** (обязательно) – константы, которые требуется присвоить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.

Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **hasBit** – установлены ли в левом операнде (в строке или числе), биты, позиции которых перечислены в правом операнде (в константе или в списке).

  Проверяемое значение переводится в двоичную систему счисления, после чего рассматривается справа налево. Проверяются символы, индекс которых указан в качестве константы или списка.

  Если проверяемое значение – это строка, то производится попытка перевести ее в целое число и обработать указанным выше способом. Если перевести строку в число невозможно, фильтр возвращает `False`.
- **hasVulnerability** – находится ли в левом операнде актив с уязвимостью и уровнем важности уязвимости, указанными в правом операнде.

  Если идентификатор и значение важности уязвимости не указаны, фильтр будет срабатывать при наличии любых уязвимостей у актива в проверяемом событии.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inDictionary** – присутствует ли в указанном словаре запись, соответствующая ключу, составленному из значений выбранных полей события.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными Kaspersky CyberTrace. Этот оператор можно использовать только на событиях, прошедших обогащение данными из Kaspersky CyberTrace, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.
- **inContextTable** – присутствует ли в указанной контекстной таблице запись.
- **intersect** – находятся ли в левом операнде элементы списка, указанные в списке в правом операнде.

Если вы хотите, чтобы оператор игнорировал регистр значений, установите флажок **без учета регистра**. Действие не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**, **hasBit** и **inDictionary**. По умолчанию флажок снят.

Вы можете изменить и удалить указанный оператор. Для изменения оператора нажмите на него и укажите новый оператор. Для удаления оператора нажмите на него и затем нажмите на клавишу **Backspace**.

e. Если вы хотите добавить группу условий для фильтра, нажмите на кнопку **Добавить группу**.

Вы можете добавить несколько групп условий.

6. Если вы выбрали вариант **Код**, укажите текстовую команду фильтра.

   В правой части конструктора отображается навигатор для перемещения по коду фильтра. Перенос строк выполняется автоматически по логическим операторам **И**, **ИЛИ**, **НЕ** или запятым, являющимися разделителем элементов списка значений.

7. Если вы хотите изменить порядок условий фильтрации, используйте значки изменения порядка ⣿. Если вы хотите удалить условие, нажмите на значок удаления ✕.

8. Нажмите **Сохранить**.

Вкладка Сервисы

Эта вкладка отображается только при изменении параметров созданного правила реагирования и используется для привязки правила к коррелляторам.

Для привязки правила реагирования к коррелятору, нажмите на кнопку **Привязать к сервису → Привязать к коррелятору**. В открывшемся окне выберите один или несколько корреляторов и нажмите **ОК**. Правило реагирования будет привязано к выбранным корреляторам и начнет выполняться в соответствии с их конфигурацией.

При необходимости вы можете отвязать правило реагирования от сервиса. Для этого нужно установить флажок рядом с нужным коррелятором, нажать **Удалить** и подтвердить удаление привязки к сервису.

Правила сбора и анализа данных

Правила сбора и анализа данных используются для обнаружения инцидентов путем анализа событий, сохраненных в базе данных Kaspersky SIEM Cloud.

В отличие от потоковой корреляции и запуска ретроспективного сканирования, правила сбора и анализа данных предусматривают предварительную обработку данных с помощью SQL-запросов (в том числе выполнение дополнительных вычислений, группировку и агрегацию через SQL) и регулярный запуск по расписанию. При наличии корректно настроенных правил сбора и анализа данных SIEM может помочь вам в обнаружении сложных атак.

Для работы с разделом вам необходимо иметь одну из следующих ролей: Главный администратор, Администратор тенанта, Аналитик первого уровня, Аналитик второго уровня.

При создании и изменении правил сбора и анализа данных требуется задать значения для параметров, указанных в таблице ниже.

Доступные параметры правила сбора и анализа данных

Параметр	Описание
Название	Обязательный параметр. Уникальное имя ресурса. Должно содержать от 1 до 128 символов в кодировке Unicode.
Тенант	Тенант, к которому будет относиться правило сбора и анализа данных.

Параметр	Описание

Sql	Обязательный параметр.
	SQL-запрос должен содержать функцию агрегации с ограничением LIMIT и/или группировку данных с ограничением LIMIT.
	Значение LIMIT должно быть от 1 до 10 000.
	Примеры SQL-запросов:
	• Запрос, содержащий только функцию агрегации:
	`SELECT count(DeviceCustomFloatingPoint1) AS `Aggregate` FROM `events` WHERE Type = 1 ORDER BY Aggregate DESC LIMIT 10`
	• Запрос, содержащий только группировку данных:
	`SELECT SourceAddress, DeviceCustomFloatingPoint1 FROM `events` WHERE Type = 1 GROUP BY SourceAddress, DeviceCustomFloatingPoint1 ORDER BY DeviceCustomFloatingPoint1 DESC LIMIT 10`
	• Запрос, содержащий функцию агрегации и группировку данных:
	`SELECT SourceAddress, sum(DeviceCustomFloatingPoint1) FROM `events` WHERE Type = 1 GROUP BY SourceAddress, DeviceCustomFloatingPoint1 ORDER BY DeviceCustomFloatingPoint1 DESC LIMIT 10`
	• Запрос, содержащий выражение из функций агрегации:
	`SELECT stddevPop(DeviceCustomFloatingPoint1) + avg(DeviceCustomFloatingPoint1) AS `Aggregate` FROM `events` WHERE Type = 1 ORDER BY Aggregate DESC LIMIT 10`
	Вы также можете использовать наборы SQL-функци `enrich` и `lookup`.

Частота запуска запроса	Обязательный параметр. Интервал выполнения SQL-запроса. Вы можете указать интервал в минутах, часах и днях. Минимальный интервал – 1 минута. Время ожидания ответа на SQL-запрос по умолчанию равно интервалу, который вы задаете в этом поле. Если выполнение SQL-запроса превышает время ожидания, возникает ошибка. В этом случае рекомендуется увеличить интервал. Например, если значение интервала равно 1 минуте, при этом запрос выполняется 80 секунд, то рекомендуется увеличить значение интервала как минимум до 90 секунд.
Теги	Необязательный параметр. Теги для поиска ресурса.
Глубина	Необязательный параметр. Выражение для определения нижней границы интервала поиска событий в базе данных. Чтобы выбрать значение из списка либо задать глубину в формате относительного интервала, установите курсор в поле. Например, если вы хотите находить все события за период, прошедший с текущего момента назад на один час, установите относительный интервал `now-1h`.
Описание	Необязательный параметр. Описание правила сбора и анализа данных.
Сопоставление	Параметры для настройки сопоставления полей результата SQL-запроса с событиями KUMA: **Исходное поле** – поле результата SQL-запроса, которое вы хотите преобразовать в событие KUMA. **Поле события** – поле события KUMA. Вы можете выбрать одно из доступных значений в списке, установив курсор мыши в это поле. **Подпись** – уникальная пользовательская метка полей событий, которые начинаются с DeviceCustom*. Вы можете добавлять новые строки таблицы и удалять строки таблицы. Для добавления новой строки таблицы нажмите на кнопку **Добавить сопоставление**. Для удаления строки установите флажок рядом с нужной строкой и нажмите на кнопку 🗑. Если вы не хотите заполнять поля вручную, вы можете нажать на кнопку **Добавить сопоставление из SQL**. Значения полей SQL запроса, включая псевдонимы (при наличии), подставятся в таблицу сопоставления полей. Например, если поле в SQL-запросе имеет значение `SourceAddress` и это значение совпадает с названием поля события, это значение проставляется в столбце **Поле события** в таблице сопоставления полей. При повторном нажатии на кнопку **Добавить сопоставление из SQL** таблица не обновляется, а значения полей SQL запроса добавляются в нее повторно.

Вы можете создавать правило сбора и анализа данных одним из следующих способов:

- В разделе **Мониторинг → Ресурсы и сервисы → Правила сбора и анализа данных**.
- В разделе **Мониторинг → Поиск угроз**.

*Чтобы создать правило сбора и анализа данных в разделе **Поиск угроз**:*

1. Создайте или сформируйте SQL-запрос и нажмите на кнопку .

   В браузере откроется новая вкладка создания правила сбора и анализа данных с предзаполненными полями **SQL запрос** и **Глубина**. Таблица сопоставления полей также будет заполнена автоматически, если в SQL-запросе вы не использовали звездочку (*).

2. Заполните обязательные поля.

   Если необходимо, вы можете изменить значение в поле **Частота запуска запроса**.

3. Сохраните параметры.

Правило сбора и анализа данных сохранено и доступно в разделе **Мониторинг → Ресурсы и сервисы → Правила сбора и анализа данных**. Чтобы правило сбора и анализа данных выполнялось, вам нужно создать для него планировщик.

Работа с правилами сбора и анализа данных

Вы можете создавать, копировать, изменять и удалять правила сбора и анализа данных.

Создание правила сбора и анализа данных

Чтобы создать правило сбора и анализа данных:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Правила сбора и анализа данных** и нажмите на кнопку **Создать**.

   Справа откроется панель создания правила сбора и анализа данных.

2. Укажите следующие параметры правила:

   a. Введите имя ресурса в поле **Название**. Имя ресурса должно быть уникальным в рамках выбранного тенанта.

   b. В раскрывающемся списке **Тенант** выберите тенант, к которому будет относиться правило сбора и анализа данных.

   c. При необходимости в раскрывающемся списке **Теги** добавьте теги.

   d. Укажите частоту запуска запроса на сбор и анализ и данных.

   e. При необходимости определите нижнюю границу периода поиска данных.

   f. При необходимости введите SQL-запрос, обязательно содержащий группировку (`GROUP BY`) или агрегационные функции и `LIMIT`. Значение `LIMIT` поддерживается для следующего количества записей: от 1 до 10 000.

3. В блоке параметров **Сопоставление** настройте сопоставление полей исходного события с полями событий. Для этого выполните следующие действия:

   a. Нажмите на кнопку **Добавить сопоставление**.

      Вы можете добавить несколько строк таблицы или удалить строки таблицы. Для удаления строки таблицы установите рядом с ней флажок и нажмите на кнопку **Удалить**.

   b. В столбце **Исходное поле** укажите название поля исходного события, которое вы хотите сопоставить с полем события Kaspersky SIEM Cloud.

   c. В столбце **Поле события** в раскрывающемся списке выберите поле события Kaspersky SIEM Cloud.

4. Нажмите **Создать**.

Правило сбора и анализа данных будет создано и доступно для использования в ресурсах.

Вы также можете создать правило сбора и анализа данных на основе SQL-запроса, который вы сформировали в разделе **Поиск угроз**. Для этого вам нужно в расположенном под полем запроса меню (⋮) выбрать **Создание правила сбора и анализа данных**. Сформированный SQL-запрос будет автоматически скопирован в открывшейся панели создания правила сбора и анализа данных.

Копирование правила сбора и анализа данных

Чтобы скопировать правило сбора и анализа данных:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Правила сбора и анализа данных** и установите флажок рядом с правилом, которое вы хотите скопировать.

2. Нажмите **Дублировать**.

   В нижней части таблицы отобразится количество выбранных правил.

   Справа откроется панель с параметрами правила сбора и анализа данных, которое вы выбрали для копирования.

   В поле **Название** отображается `<название выбранного правила> - копия`.

3. Измените нужные параметры (см. инструкцию по созданию правила сбора и анализа данных).

4. Нажмите **Сохранить**.

Копия правила сбора и анализа данных будет создана.

Изменение параметров правила сбора и анализа данных

Чтобы изменить правило сбора и анализа данных:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Правила сбора и анализа данных** и нажмите на правило, которое вы хотите изменить.

   Справа откроется панель с параметрами выбранного правила сбора и анализа данных.

2. Измените нужные параметры.

3. Выполните одно из следующих действий:

   - Нажмите **Сохранить**, чтобы сохранить изменения.

   - Нажмите **Сохранить с комментарием** и в открывшемся окне укажите комментарий к внесенным изменениям. Изменения будут сохранены, и комментарий будет добавлен к созданной версии правила сбора и анализа данных.

Правило сбора и анализа данных будет обновлено.

Удаление правила сбора и анализа данных

Чтобы удалить правило сбора и анализа данных:

1. В веб-консоли перейдите в раздел **Мониторинг → Ресурсы и сервисы → Правила сбора и анализа данных** и установите флажок рядом с правилом, которое вы хотите удалить.

   В нижней части таблицы отобразится количество выбранных ресурсов.

2. Нажмите **Удалить**.

3. В открывшемся окне подтвердите удаление.

Правило сбора и анализа данных и все его сохраненные версии будут удалены.

Настройка планировщика для правила сбора и анализа данных

Чтобы правило сбора и анализа данных выполнялось, вам нужно создать для него планировщик.

Планировщик направляет SQL-запросы в заданные вами разделы хранилища с интервалом и глубиной поиска, который вы настраиваете в правиле, а затем преобразует результаты SQL-запросов в базовые события и направляет в коррелятор.

> Результаты SQL-запросов, преобразованные в базовые события, не попадают в хранилище.

Для корректной работы планировщика необходимо настроить связь между правилом сбора и анализа данных, хранилищем и корреляторами в разделе **Мониторинг → Ресурсы и сервисы → Сбор и анализ данных**.

Для работы с разделом вам нужно иметь одну из следующих ролей: Главный администратор, Администратор тенанта, Аналитик 2-го уровня, Чтение общих ресурсов, Редактирование общих ресурсов.

Планировщики расположены в таблице по дате последнего запуска. Вы можете сортировать данные в столбцах по возрастанию и убыванию, нажав на значок стрелки вниз (⌄) в заголовке столбца.

Доступные столбцы таблицы планировщиков:

- **Название правила** – название правила сбора и анализа данных, для которого вы создали планировщик.
- **Название тенанта** – название тенанта, которому принадлежит правило сбора и анализа данных.
- **Состояние** – статус планировщика. Возможны следующие значения:
  - **Включено** – планировщик выполняется, правило сбора и анализа данных будет запускаться по заданному расписанию.
  - **Выключено** – планировщик не выполняется.

    Этот статус планировщик имеет по умолчанию при создании. Чтобы планировщик выполнялся, необходимо перевести его в состояние **Включено**.
- **Планировщик завершил работу в** – время последнего запуска правила сбора и анализа данных, для которого вы создали планировщик.
- **Статус выполнения правила** – статус, с которым планировщик завершил работу. Возможны следующие значения:
  - **Ok** – планировщик завершил работу без ошибок, правило выполнено.
  - **Неизвестно** – планировщик переведен в состояние **Включено**, и его статус в данный момент неизвестен. Статус **Неизвестно** отображается, если вы привязали хранилища и корреляторы на соответствующих вкладках и перевели планировщик в состояние **Включено**, но еще не запустили.
  - **Остановлен** – планировщик остановлен, правило не выполняется.
  - **Ошибка** – планировщик завершил работу, правило выполнено с ошибкой.
- **Последняя ошибка** – ошибки (при наличии), которые возникли при выполнении правила сбора и анализа данных.

> Неуспешная попытка отправки событий в установленный коррелятор не является ошибкой.

На панели инструментов в верхней части таблицы вы можете выполнять действия над планировщиками.

Доступные действия

- Добавить новый планировщик. Нажмите на кнопку **Добавить** и в отобразившемся окне установите флажки рядом с названиями правил сбора и анализа данных, для которых вы хотите создать планировщик.

  > В этом окне вы можете выбрать правило сбора и анализа данных только из ранее созданных. Создать новое правило нельзя.

- Удалить планировщик. В таблице планировщиков установите флажки рядом планировщиками, которые вы хотите удалить, и нажмите на кнопку **Удалить**. Планировщик и привязки удаляются. Правило сбора и анализа данных не удаляется.

- Включить планировщик. В таблице планировщиков установите флажки рядом планировщиками, которые вы хотите включить, и нажмите на кнопку **Включить по расписанию**. Правило сбора и анализа данных, для которого был создан этот планировщик, будет выполняться согласно расписанию, заданному в настройках этого правила.

- Отключить планировщик. В таблице планировщиков установите флажки рядом планировщиками, которые вы хотите отключить, и нажмите на кнопку **Отключить**. Правило сбора и анализа данных временно перестает выполняться, при этом сам планировщик и привязки не удаляются.

- Запустить планировщик. В таблице планировщиков установите флажки рядом с включенными планировщиками, и нажмите на кнопку **Запустить сейчас**. Правило сбора и анализа данных, для которого был создан этот планировщик, выполнится немедленно.

Чтобы изменить параметры планировщика, нажмите на соответствующую строку в таблице.

Доступные параметры планировщика для правил сбора и анализа данных описаны ниже.

Вкладка Общие

На этой вкладке вы можете выполнить следующие действия:

- Включить или выключить планировщик с помощью переключателя.

  Если переключатель включен, правило сбора и анализа данных будет запускаться по расписанию, заданному в его настройках.

- Изменить следующие параметры правила сбора и анализа данных:

  - Название
  - Частота запуска запроса
  - Глубина
  - Sql
  - Описание
  - Сопоставление

Вкладка Привязанные хранилища

На этой вкладке вам нужно задать хранилище, в которое планировщик будет направлять SQL-запросы.

Чтобы задать хранилище:

1. Нажмите на кнопку **Привязать** на панели инструментов.
2. В открывшемся окне укажите название хранилища, к которому вы хотите добавить привязку, а также название раздела выбранного хранилища.

   Вы можете выбрать только одно хранилище, но несколько разделов этого хранилища.

3. Нажмите на кнопку **Добавить**.

Привязка создана и отображается в таблице на вкладке **Привязанные хранилища**.

При необходимости вы можете удалить привязки, установив флажки в соответствующих строках таблицы и нажав на кнопку **Отвязать выбранные**.

Вкладка Привязанные коррелляторы

На этой вкладке вам нужно добавить коррелляторы для работы с базовыми событиями.

Чтобы добавить коррелятор:

1. Нажмите на кнопку **Привязать** на панели инструментов.
2. В открывшемся окне установите курсор мыши в поле **Коррелятор**.
3. В отобразившемся списке коррелляторов установите флажки рядом с коррелляторами, которые вы хотите добавить.
4. Нажмите на кнопку **Добавить**.

Коррелляторы добавлены и отображаются в таблице на вкладке **Привязанные коррелляторы**.

При необходимости вы можете удалить коррелляторы, установив флажки в соответствующих строках таблицы и нажав на кнопку **Отвязать выбранные**.

Также вы можете просмотреть результат работы планировщика в журнале Ядра, предварительно настроив режим **Отладка** в параметрах Ядра. Чтобы скачать журнал, выберите раздел Kaspersky SIEM Cloud **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**, затем выберите сервис Ядра и нажмите на кнопку **Журнал.**

Записи с результатом работы планировщика имеют приставку `datamining scheduler`.

Анализ объемов сетевого трафика

При получении событий в формате NetFlow возникает необходимость в анализе объемов сетевого трафика между хостами. Подсчет трафика между хостами можно выполнять с помощью правил корреляции, но большое количество обращений к активным листам делает такой подход малоэффективным.

Для анализа объемов сетевого трафика мы рекомендуем использовать правила сбора и анализа данных (англ. Data mining), которые позволяют получить данные по трафику и выявить закономерности в массиве событий в формате NetFlow.

Следуя этому сценарию, вы можете создать правило сбора и анализа данных для подсчета сетевого трафика. Для каждого этапа приведены ссылки на инструкции по выполнению необходимых действий и дополнительные материалы для ознакомления.

1 Создание правила сбора и анализа данных

Создайте правило сбора и анализа данных для анализа трафика между хостами со следующими параметрами поискового SQL-запроса:

- Группировка (`GROUP BY`) осуществляется по параметрам `SourceAddress` и `DestinationAddress`.
- Агрегация выполняется по полям (например, `SUM(BytesIn + BytesOut) AS TotalTraffic`).
- Частота запуска правила сбора и анализа данных – один час.
- Глубина поискового запроса – один час.

  Если вы хотите проанализировать сетевой трафик за другой период, вам нужно указать этот период.
- Максимальное количество событий для анализа (`LIMIT`) – 10000.

В блоке параметров **Сопоставление** нужно также указать значения параметров для настройки сопоставления полей результата SQL-запроса с событиями Kaspersky SIEM Cloud. Вы можете сделать это, нажав на кнопку **Добавить сопоставление из SQL**.

> При использовании параметра для агрегированного выражения (`AS`) вам нужно указать значение вручную. Например, для параметра `TotalTraffic` в поле **Исходное поле** в **Поле события** укажите `DeviceCustomNumber1`.

Пример поискового SQL-запроса

```
SELECT SourceAddress, DestinationAddress, SUM(BytesIn + BytesOut) AS TotalTraffic
FROM 'events'
GROUP BY SourceAddress, DestinationAddress
LIMIT 10000
```

2 Привязка правила сбора и анализа данных к сервисам

После создания правила сбора и анализа данных выполните следующие действия:

1. Добавьте правило в планировщик, привязав к правилу сбора и анализа данных хранилище и коррелятор.
2. С помощью переключателя включите использование созданного правила для анализа трафика между хостами.

   По умолчанию переключатель выключен.

3 Создание правила корреляции

После привязки правила сбора и анализа данных создайте правило корреляции, которое будет использоваться в привязанном корреляторе. При создании правила вам нужно учитывать следующее:

- На вкладке **Общие** в раскрывающемся списке **Группирующие поля** выберите все значения используемые в правиле сбора и анализа данных параметры (`SourceAddress`, `DestinationAddress`, `DeviceCustomNumber1`).

- На вкладке **Селекторы** в конструкторе параметров фильтра нужно указать значение в байтах, которое используется для определения максимального объема трафика за выбранную единицу времени. Например, если вы хотите определить объем трафика 1 ГБ, нужно указать следующее:

  ```
  DeviceCustomNumber1 ≥ 1073741824
  ```

- На вкладке **Действия** с помощью флажка нужно выбрать **В дальнейшую обработку**.

В результате выполнения указанных в этом сценарии действий Ядро Kaspersky SIEM Cloud аккумулирует информацию по событиям в решении и направляет ее в коррелятор, где применяется правило корреляции. Если трафик за один час превышает установленное значение, решение создает алерт.

Устранение неисправностей

Известные проблемы и ограничения

Kaspersky SIEM Cloud имеет ряд не критичных ограничений:

- Темная тема поддерживается частично. Некоторые разделы и элементы интерфейса продолжают отображаться в светлой теме, даже если выбрана темная тема.
- Kaspersky SIEM Cloud недоступен для рабочих областей, созданных в регионе Мексика. Более подробная информация о регионах рабочих областей в документации Kaspersky Security Center Cloud Console.
- В настоящее время невозможно одновременно активировать и использовать несколько облачных решений.
- В текущей версии решения названия категорий трудозатрат доступны только на русском языке. Перевод доступных категорий в следующей таблице:

ru-RU	en-US
Создание и оптимизация плейбуков	Playbooks creation and optimization
Мониторинг и обработка алертов	Alerts monitoring and processing
Расследование и реагирование на инциденты	Investigation and incident response
Отчетность и пост-анализ	Reporting and post-analysis
Проактивный поиск угроз	Threat Hunting
Обучение и поддержка команды	Training and team support

- Сканирование YARA и работа с YARA-правилами не поддерживается.
- Если пользователь попытается войти в веб-консоль из региона, отличного от того, в котором была создана его рабочая область, он не сможет просмотреть разделы, доступные в активированном решении (алерты, инциденты, угрозы и так далее). Вместо этого пользователь получит уведомление с предложением перейти в веб-консоль своего региона для доступа к этим разделам.
- Kaspersky SIEM Cloud не поддерживает использование коллекторов, основанных на протоколе UDP, включая NetFlow, sFlow и SNMP Trap.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky SIEM Cloud, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky SIEM Cloud.

Kaspersky предоставляет поддержку Kaspersky SIEM Cloud в течение жизненного цикла (см. страницу жизненного цикла приложений). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки.

Журналы Kaspersky SIEM Cloud

По умолчанию для всех компонентов Kaspersky SIEM Cloud в журнале регистрируются только ошибки. Чтобы получать детализированные данные в журналах, следует настроить в параметрах компонента режим **Отладка**.

Журнал пополняется, пока не достигнет размера 5 ГБ. По достижении 5 ГБ журнал архивируется и события начинают записываться в новый журнал. Архивы хранятся в папке с журналами в течение 7 дней, по истечении 7 дней архив удаляется. Одновременно на сервере хранится не более четырех заархивированных журналов. При появлении нового архива журнала, если архивов становится больше четырех, самый давний архив удаляется.

Режим **Отладка** доступен для следующих компонентов:

Сервисы:

- Хранилище
- Корреляторы
- Коллекторы
- Агенты

Как включить: в параметрах сервиса с помощью переключателя **Отладка**.

Где хранятся: в директории установки сервиса. Например, `/opt/kaspersky/kuma/<service_name>/log/<service_name>`. Журналы событий сервисов можно скачать в веб-консоли в разделе **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы**. Для этого вам нужно выбрать нужный сервис, нажать на значок меню (⋮) и выбрать **Скачать** → **Скачать журнал**.

В открывшемся окне в раскрывающемся списке **Период** нужно выбрать период для экспорта данных из журнала сервиса одним из следующих способов:

- Если вы хотите указать точную дату, в календаре слева выберите даты начала и окончания периода и нажмите на кнопку **Применить**.

  Вы можете выбрать дату до текущей включительно. Формат даты и времени зависит от параметров вашего браузера. Если в поле **Дата от** или **Дата до** есть значение и вы не меняли вручную значение времени, при выборе даты в календаре в поле **Дата от** автоматически подставится время 00:00:00.000, а в поле **Дата до** – 23:59:59.999. Если вы вручную удалили значение в поле **Дата от** или **Дата до**, при выборе даты в календаре в поле автоматически подставится текущее время. После того как вы выберите значение в одном из полей, фокус переключается на другое поле. Если в поле **Дата до** вы выбираете значение, которое меньше значения в поле **Дата от**, это меньшее значение будет автоматически подставлено в поле **Дата от**.

- Если вы хотите указать относительный период, выберите один из доступных периодов в списке **Относительный период** справа.

  Период рассчитывается относительно настоящего времени.

- Если вы хотите задать пользовательский период, укажите или измените значение вручную в полях **Дата от** и **Дата до**.

  Вы можете указать точные дату и время в формате **DD.MM.YYYY HH:mm:ss.SSS** для русской локализации и **YYYY-MM-DD HH:mm:ss.SSS** для английской локализации или период относительно текущего времени в виде формулы. При необходимости вы также можете комбинировать эти способы. Если при вводе точной даты вы не указали миллисекунды, значение 000 подставляется автоматически. Если вы вручную изменили время в полях **Дата от** или **Дата до**, при переключении даты в календаре значение времени не меняется.

  В формулах относительного периода используйте параметр **now** для обозначения текущих даты и времени, а также: символы "+" (только в поле **Дата до**), "-", "/" (округление до ближайшего) и единицы изменения времени **y** (год), **M** (месяц), **w** (неделя), **d** (день), **h** (час), **m** (минута), **s** (секунда). Например, вы можете указать период **now-5d**, чтобы получить данные за последние пять дней, или **now/w**, чтобы получить данные с начала первого дня текущей недели (00:00:00:000 в UTC) до текущего времени **now**.

  > Поле **Дата от** является обязательным, и его значение не может превышать значение, установленное в поле **Дата до**, а также не может быть меньше 01.01.1970 (при указании точной даты или относительного периода). Значение в поле **Дата до** не должно быть меньше значения, установленного в поле **Дата от**. Если вы не укажете значение в поле **Дата до**, параметр **now** указывается автоматически.

  По умолчанию выбран относительный период **1 день (now-1d)**. Границы периода включаются. Например, для периода **Сегодня** отобразятся события с начала сегодняшнего дня 00:00:00:000 до текущего времени **now** включительно, а для периода **Вчера** – с начала вчерашнего дня 00:00:00:000 до 00:00:00:000 сегодняшнего дня.

  Время в Kaspersky SIEM Cloud хранится в UTC, но в интерфейсе оно конвертируется в соответствии с часовым поясом вашего браузера. Это нужно учитывать для относительных периодов **Сегодня**, **Вчера**, **Эта неделя** и **Этот месяц**. Например, если в браузере установлен часовой пояс UTC+3 и вы выбрали период отображения данных **Сегодня**, данные будут отображаться за период с 03:00:00.000 до текущего времени, а не с 00:00:00.000.

  Если при выборе относительного периода **Сегодня**, **Вчера**, **Эта неделя** или **Этот месяц** вы хотите отобразить данные в соответствии с вашим часовым поясом, вам нужно вручную добавить сдвиг по времени в поля **Дата от** и **Дата до** (если указано значение кроме now), прибавив или убавив необходимое количество часов. Например, если в браузере установлен часовой пояс UTC+3 и вы хотите отобразить данные за период **Вчера**, вам нужно изменить значение в поле **Дата от** на **now-1d/d-3h**, а в поле **Дата до** – на **now/d-3h**. Если же вы хотите отобразить данные за период **Сегодня**, вам нужно изменить значение только в поле **Дата от** на **now/d-3h**.

  > Если вам нужны результаты до 23:59:59:999 вчерашнего дня в UTC, то используйте SQL-запрос с фильтром по Timestamp или укажите точные дату и время.

После настройки периода нужно нажать на кнопку **Скачать**. Скачиваемый файл может содержать не более 10 000 последних строк журнала за выбранный период.

Журналы на машинах Linux можно просмотреть с помощью команды `journalctl` и `tail`. Например:

- Коллекторы. Чтобы вернуть последние журналы определенного коллектора, установленного на сервере, выполните команду:

  ```
  journalctl -f -u kuma-collector-<collector_ID>
  ```

	• Агенты. Чтобы вернуть последние журналы агента, установленного на сервере, выполните команду: `tail -f /opt/kaspersky/agent/<agent_ID>/log/agent` Активность агентов на устройствах под управлением Windows всегда регистрируется, если им назначено разрешение на вход в систему в качестве сервиса. Данные указываются более подробно, если включен переключатель **Отладка**. Журналы агентов на машинах Windows можно просмотреть в файле `%PROGRAMDATA%\Kaspersky Lab\KUMA\<agent_ID>\agent.log`. Журналы агентов на машинах Linux хранятся в директории установки агента.
Ресурсы: • Коннекторы • Точки назначения • Правила обогащения	Как включить: в параметрах сервиса, к которому привязан ресурс, с помощью переключателя **Отладка**. Где хранятся: журналы хранятся на машине, на которой установлен сервис, использующий нужный ресурс. Детализированные данные для ресурсов можно посмотреть в журнале сервиса, к которому привязан ресурс.

Приложения

В этом разделе представлены приложения к основному тексту документа.

Модель данных нормализованного события

В этом разделе вы можете найти модель данных нормализованного события KUMA. Все события, которые обрабатываются коррелеторами KUMA с целью обнаружения алертов, должны соответствовать этой модели.

События, несовместимые с этой моделью данных, необходимо импортировать в этот формат (нормализовать) с помощью коллекторов.

Модель данных нормализованного события

Название поля	Тип данных	Размер поля	Описа
Назначение данных полей определено в названии поля. Поля доступны для изменения.			
ApplicationProtocol	Строка	31 символов	Название протокола прикладного уровня. Например, HTTPS,
BytesIn	Число	От -9223372036854775808 до 9223372036854775807	Количество полученных байт.
BytesOut	Число	От -9223372036854775808 до 9223372036854775807	Количество отправленных байт.
DestinationAddress	Строка	45 символов	IPv4 или IPv6-адрес актива, с которым будет выполнено дейс xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
DestinationCity	Строка	1023 символов	Город, соответствующий IP-адресу из поля DestinationAddre
DestinationCountry	Строка	1023 символов	Страна, соответствующая IP-адресу из поля DestinationAdd
DestinationDnsDomain	Строка	255 символов	DNS-часть полного доменного имени точки назначения.
DestinationHostName	Строка	1023 символов	Название устройства точки назначения. FQDN точки назначе
DestinationLatitude	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Долгота, соответствующая IP-адресу из поля DestinationAdc
DestinationLongitude	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Широта, соответствующая IP-адресу из поля DestinationAdc
DestinationMacAddress	Строка	17 символов	MAC-адрес точки назначения. Например, aa:bb:cc:dd:ee:00
DestinationNtDomain	Строка	255 символов	Windows Domain Name точки назначения.
DestinationPort	Число	От -9223372036854775808 до 9223372036854775807	Номер порта точки назначения.
DestinationProcessID	Число	От -9223372036854775808 до 9223372036854775807	Идентификатор системного процесса, зарегистрированный
DestinationProcessName	Строка	1023 символов	Название системного процесса, зарегистрированного на то
DestinationRegion	Строка	1023 символов	Регион, соответствующий IP-адресу из поля DestinationAddr

DestinationServiceName	Строка	1023 символов	Название сервиса или службы на стороне точки назначения
DestinationTranslatedAddress	Строка	45 символов	IPv4 или IPv6-адрес точки назначения после трансляции. Нап
DestinationTranslatedPort	Число	От -9223372036854775808 до 9223372036854775807	Номер порта на точке назначения после трансляции.
DestinationUserID	Строка	1023 символов	Идентификатор пользователя точки назначения.
DestinationUserName	Строка	1023 символов	Имя пользователя точки назначения.
DestinationUserPrivileges	Строка	1023 символов	Названия ролей, которые идентифицируют пользовательски Administrator и т.п.
DeviceAction	Строка	63 символов	Действие, которое было предпринято источником события.
DeviceAddress	Строка	45 символов	IPv4 или IPv6-адрес устройства, с которого было получено с xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
DeviceCity	Строка	1023 символов	Город, соответствующий IP-адресу из поля DeviceAddress.
DeviceCountry	Строка	1023 символов	Страна, соответствующая IP-адресу из поля DeviceAddress.
DeviceDnsDomain	Строка	255 символов	DNS-часть полного доменного имени устройства, с которого
DeviceEventClassID	Строка	1023 символов	Идентификатор типа события, присвоенный источником соб
DeviceExternalID	Строка	255 символов	Идентификатор устройства или приложения, присвоенный и
DeviceFacility	Строка	1023 символов	Значение параметра facility, установленное источником соб
DeviceHostName	Строка	100 символов	Имя устройства, с которого было получено событие. FQDN у
DeviceInboundinterface	Строка	128 символов	Название интерфейса входящего соединения.
DeviceLatitude	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Долгота, соответствующая IP-адресу из поля DeviceAddress
DeviceLongitude	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Широта, соответствующая IP-адресу из поля DeviceAddress
DeviceMacAddress	Строка	17 символов	MAC-адрес актива, с которого было получено событие. Напр
DeviceNtDomain	Строка	255 символов	Windows Domain Name устройства.
DeviceOutboundinterface	Строка	128 символов	Название интерфейса исходящего соединения.
DevicePayloadID	Строка	128 символов	Уникальный идентификатор полезной нагрузки (Payload), кот
DeviceProcessID	Число	От -9223372036854775808 до 9223372036854775807	Идентификатор системного процесса на устройстве, которо
DeviceProcessName;	Строка	1023 символов	Название процесса.
DeviceProduct	Строка	63 символов	Название приложения, сформировавшего событие. DeviceVe идентифицируют источник журнала.
DeviceReceiptTime	Число	От -9223372036854775808 до 9223372036854775807	Время получения события устройством.
DeviceRegion	Строка	1023 символов	Регион, соответствующий IP-адресу из поля DeviceAddress.
DeviceTimeZone	Строка	255 символов	Временная зона устройства, на котором было создано собы
DeviceTranslatedAddress	Строка	45 символов	Ретранслированный IPv4 или IPv6-адрес устройства, с котор xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
DeviceVendor	Строка	63 символов	Название производителя источника события. DeviceVendor, идентифицируют источник журнала.
DeviceVersion	Строка	31 символов	Версия приложения источника события. DeviceVendor, Devic источник журнала.

EndTime	Число	От -9223372036854775808 до 9223372036854775807	Дата и время (timestamp) завершения события.
EventOutcome	Строка	63 символов	Результат выполнения операции. Например, success, failure.
ExternalID	Строка	40 символов	Поле в которое может быть сохранен идентификатор.
FileCreateTime	Число	От -9223372036854775808 до 9223372036854775807	Время создания файла.
FileHash	Строка	255 символов	Хеш-сумма файла. Пример: CA737F1014A48F4C0B6DD43CB177B0AFD9E5169367544C49
FileID	Строка	1023 символов	Значение идентификатора файла.
FileModificationTime	Число	От -9223372036854775808 до 9223372036854775807	Время последнего изменения файла.
FileName	Строка	1023 символов	Имя файла, без указания пути к файлу.
FilePath	Строка	1023 символов	Путь к файлу, включая имя файла.
FilePermission	Строка	1023 символов	Список разрешений файла.
FileSize	Число	От -9223372036854775808 до 9223372036854775807	Размер файла.
FileType	Строка	1023 символов	Тип файла.
Message	Строка	1023 символов	Краткое описание события.
Имя	Строка	512 символов	Название события.
OldFileCreateTime	Число	От -9223372036854775808 до 9223372036854775807	Время создания OLD-файла из события. Время указывается часовому поясу браузера пользователя.
OldFileHash	Строка	255 символов	Хеш-сумма OLD-файла. Пример: CA737F1014A48F4C0B6DD43CB177B0AFD9E5169367544C49
OldFileID	Строка	1023 символов	Идентификатор OLD-файла.
OldFileModificationTime	Число	От -9223372036854775808 до 9223372036854775807	Время последнего изменения OLD-файла.
OldFileName	Строка	1023 символов	Имя OLD-файла (без пути).
OldFilePath	Строка	1023 символов	Путь к OLD-файлу, включая имя файла.
OldFilePermission	Строка	1023 символов	Список разрешений OLD-файла.
OldFileSize	Число	От -9223372036854775808 до 9223372036854775807	Размер OLD-файла.
OldFileType	Строка	1023 символов	Тип OLD-файла.
Reason	Строка	1023 символов	Информация о причине возникновения события.
RequestClientApplication	Строка	1023 символов	Значение параметра "user-agent" http-запроса.
RequestContext	Строка	2048 символов	Описание контекста http-запроса.
RequestCookies	Строка	1023 символов	Cookies, связанные с http-запросом.
RequestMethod	Строка	1023 символов	Метод, который использовался при выполнении http-запрос
RequestUrl	Строка	1023 символов	Запрошенный URL.
Severity	Строка	1023 символов	Критичность. Это может быть поле Severity или поле Level с

SourceAddress	Строка	45 символов	IPv4 или IPv6-адрес источника. Пример формата: 0.0.0.0 или
SourceCity	Строка	1023 символов	Город, соответствующий IP-адресу из поля SourceAddress.
SourceCountry	Строка	1023 символов	Страна, соответствующая IP-адресу из поля SourceAddress.
SourceDnsDomain	Строка	255 символов	DNS-часть полного доменного имени источника.
SourceHostName	Строка	1023 символов	Доменное имя Windows-устройства источника события.
SourceLatitude	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Долгота, соответствующая IP-адресу из поля SourceAddress
SourceLongitude	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Широта, соответствующая IP-адресу из поля SourceAddress
SourceMacAddress	Строка	17 символов	MAC-адрес источника. Пример формата: aa:bb:cc:dd:ee:00
SourceNtDomain	Строка	255 символов	Windows Domain Name источника.
SourcePort	Число	От -9223372036854775808 до 9223372036854775807	Номер порта источника.
SourceProcessID	Число	От -9223372036854775808 до 9223372036854775807	Идентификатор системного процесса.
SourceProcessName	Строка	1023 символов	Название системного процесса на источнике. Например, ssh
SourceRegion	Строка	1023 символов	Регион, соответствующий IP-адресу из поля SourceAddress.
SourceServiceName	Строка	1023 символов	Название сервиса или службы на стороне источника. Напри
SourceTranslatedAddress	Строка	15 символов	IPv4 или IPv6-адрес источника после трансляции. Пример фо
SourceTranslatedPort	Число	От -9223372036854775808 до 9223372036854775807	Номер порта на источнике после трансляции.
SourceUserID	Строка	1023 символов	Идентификатор пользователя источника.
SourceUserName	Строка	1023 символов	Имя пользователя источника.
SourceUserPrivileges	Строка	1023 символов	Названия ролей, которые идентифицируют пользовательски Administrator и т.п.
StartTime	Число	От -9223372036854775808 до 9223372036854775807	Дата и время (timestamp) в которые, началась активность, св
Tactic	Строка	128 символов	Название тактики из матрицы MITRE ATT&CK.
Technique	Строка	128 символов	Название техники из матрицы MITRE ATT&CK.
TransportProtocol	Строка	31 символов	Название протокола Транспортного уровня сетевой модели
Тип.	Число	От -9223372036854775808 до 9223372036854775807	Тип события: 1 – базовое, 2 - агрегированное, 3 - корреляцио
Поля, назначение которых может быть определено пользователем. Поля доступны для измен			
DeviceCustomDate1	Число, timestamp	От -9223372036854775808 до 9223372036854775807	Поле для маппинга значения даты и времени (timestamp). Вр отображается по часовому поясу браузера пользователя.
DeviceCustomDate1Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomDate1.
DeviceCustomDate2	Число, timestamp	От -9223372036854775808 до 9223372036854775807	Поле для маппинга значения даты и времени (timestamp). Вр отображается по часовому поясу браузера пользователя.

DeviceCustomDate2Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomDate2.
DeviceCustomFloatingPoint1	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Поле для маппинга чисел с плавающей точкой.
DeviceCustomFloatingPoint1Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomFloatingPo
DeviceCustomFloatingPoint2	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Поле для маппинга чисел с плавающей точкой.
DeviceCustomFloatingPoint2Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomFloatingPo
DeviceCustomFloatingPoint3	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Поле для маппинга чисел с плавающей точкой.
DeviceCustomFloatingPoint3Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomFloatingPo
DeviceCustomFloatingPoint4	Число с плавающей точкой	От +/- 1.7E-308 до 1.7E+308	Поле для маппинга чисел с плавающей точкой.
DeviceCustomFloatingPoint4Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomFloatingPo
DeviceCustomIPv6Address1	Строка	45 символов	Поле для маппинга значения IPv6 address. Пример формата:
DeviceCustomIPv6Address1Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomIPv6Addre
DeviceCustomIPv6Address2	Строка	45 символов	Поле для маппинга значения IPv6 address. Пример формата:
DeviceCustomIPv6Address2Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomIPv6Addre
DeviceCustomIPv6Address3	Строка	45 символов	Поле для маппинга значения IPv6 address. Пример формата:
DeviceCustomIPv6Address3Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomIPv6Addre
DeviceCustomIPv6Address4	Строка	45 символов	Поле для маппинга значения IPv6 address. Например, y:y:y:y:y:y
DeviceCustomIPv6Address4Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomIPv6Addre
DeviceCustomNumber1	Число	От -9223372036854775808 до 9223372036854775807	Поле для маппинга целочисленного значения.
DeviceCustomNumber1Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomNumber1.
DeviceCustomNumber2	Число	От -9223372036854775808 до 9223372036854775807	Поле для маппинга целочисленного значения.
DeviceCustomNumber2Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomNumber2.
DeviceCustomNumber3	Число	От -9223372036854775808 до 9223372036854775807	Поле для маппинга целочисленного значения.
DeviceCustomNumber3Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomNumber3.
DeviceCustomString1	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString1Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomString1.
DeviceCustomString2	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString2Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomString2.
DeviceCustomString3	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString3Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomString3.
DeviceCustomString4	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString4Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomString4.
DeviceCustomString5	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString5Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomString5.

DeviceCustomString6	Строка	4000 символов	Поле для маппинга строкового значения.
DeviceCustomString6Label	Строка	1023 символов	Поле для описания назначения поля DeviceCustomString6.
DeviceDirection	Число	От -9223372036854775808 до 9223372036854775807	Поле для описания направления соединения события. "0" - вх
DeviceEventCategory	Строка	1023 символов	Категория события, присвоенная устройством, направившим
FlexDate1	Число, timestamp	От -9223372036854775808 до 9223372036854775807	Поле для маппинга значения даты и времени (timestamp). Вр отображается по часовому поясу браузера пользователя.
FlexDate1Label	Строка	128 символов	Поле для описания назначения поля FlexDate1Label.
FlexNumber1	Число	От -9223372036854775808 до 9223372036854775807	Поле для маппинга целочисленного значения.
FlexNumber1Label	Строка	128 символов	Поле для описания назначения поля FlexNumber1Label.
FlexNumber2	Число	От -9223372036854775808 до 9223372036854775807	Поле для маппинга целочисленного значения.
FlexNumber2Label	Строка	128 символов	Поле для описания назначения поля FlexNumber2Label.
FlexString1	Строка	1023 символов	Поле для маппинга строкового значения.
FlexString1Label	Строка	128 символов	Поле для описания назначения поля FlexString1Label.
FlexString2	Строка	1023 символов	Поле для маппинга строкового значения.
FlexString2Label	Строка	128 символов	Поле для описания назначения поля FlexString2Label.
Служебные поля. Недоступны для редактирования.			
AffectedAssets	Вложенная структура [Affected]	-	Вложенная структура, из которой можно обратиться к связа узнать, сколько раз они фигурируют в событиях алерта.
AggregationRuleID	Строка	-	Идентификатор агрегационного правила.
AggregationRuleName	Строка	-	Название агрегационного правила, которое обработало соб
BaseEventCount	Число	-	Для агрегированного базового события – количество базов правилом. Для корреляционного события – это количество б корреляционным правилом, которое создало корреляционно
BaseEvents	Вложенный список [Event]	-	Вложенная структура со списком базовых событий. Поле мо
Code	Строка	-	В базовом событии это код возврата процесса, функции или
CorrelationRuleID	Строка	-	ID корреляционного правила.
CorrelationRuleName	Строка	-	Название корреляционного правила, в результате срабатыва Заполняется только для корреляционных событий.
DestinationAccountID	Строка	-	Поле хранит идентификатор пользователя.
DestinationAssetID	Строка	-	Поле хранит идентификатор актива точки назначения.
DeviceAssetID	Строка	-	Поле хранит идентификатор актива, направившего событие
Extra	Вложенный словарь [строка:строка]	-	Поле, в которое во время нормализации сырого события мо сопоставление с полями события KUMA. Это поле может бы размер поля – 4 МБ.
GroupedBy	Строка	-	Список названия полей, по которым была группировка в корр корреляционного события.
ID	Строка	-	Уникальный идентификатор события типа UUID. Для базового генерирует коллектор. Идентификатор корреляционного соб меняет своего значения.
Raw	Строка	-	Не нормализованный текст исходного "сырого" события. Мак

ReplayID	Строка	-	Идентификатор ретроспективной проверки, в процессе кото
ServiceID	Строка	-	Идентификатор экземпляра сервиса: коррелятора, коллекто
ServiceName	Строка	-	Название экземпляра микросервиса, которое присваивает а
SourceAccountID	Строка	-	Поле хранит идентификатор пользователя.
SourceAssetID	Строка	-	Поле хранит идентификатор актива источника событий.
SpaceID	Строка	-	Идентификатор пространства.
TenantID	Строка	-	Поле хранит идентификатор тенанта.
TI	Вложенный словарь [строка:строка]	-	Поле, в котором в формате словаря содержатся категории, п индикаторам из события.
TICategories	map[String]	-	Поле, содержит категории, полученные от внешнего TI-поста
Timestamp	Число	-	Время создания базового события на коллекторе. Время со указывается в UTC0. В Консоли KUMA значение отображает

Вложенная структура `Affected`

Поле	Тип данных	Описание
`Assets`	Вложенный список `[AffectedRecord]`	Перечень и количество связанных с алертом активов.
`Accounts`	Вложенный список `[AffectedRecord]`	Перечень и количество связанных с алертом учетных записей.

Вложенная структура `AffectedRecord`

Поле	Тип данных	Описание
`Значение`	Строка	Идентификатор актива или учетной записи.
`Count`	Число	Количество раз актив или учетная запись фигурирует в связанных с алертом событиях.

Поля, формируемые Kaspersky SIEM Cloud

Kaspersky SIEM Cloud формирует следующие поля, не подлежащие изменениям: BranchID, BranchName, DestinationAccountName, DestinationAssetName, DeviceAssetName, SourceAccountName, SourceAssetName, TenantName.

Настройка модели данных нормализованного события из KATA EDR

Для расследования данных необходимо, чтобы идентификаторы события и процесса KATA/EDR попадали в определенные поля нормализованного события. Для построения дерева процессов для событий, поступающих из KATA/EDR, необходимо настроить копирование данных из полей сырых событий в поля нормализованного события в нормализаторах в Kaspersky SIEM Cloud следующим образом:

1. Для любых событий KATA/EDR должна быть настроена нормализация с копированием следующих полей:

   - поле события KATA/EDR `EventType` должно копироваться в поле нормализованного события Kaspersky SIEM Cloud `DeviceEventCategory`;

   - поле события KATA/EDR `HostName` должно копироваться в поле нормализованного события Kaspersky SIEM Cloud `DeviceHostName`.

2. Для любого события, где поле DeviceProduct = 'KATA' должна быть настроена нормализация в соответствии таблице ниже.

   Нормализация полей событий из KATA/EDR

Поле в событии KATA/EDR	Поле нормализованного события
IOATag	DeviceCustomIPv6Address2
	IOATag
IOAImportance	DeviceCustomIPv6Address1
	IOAImportance
FilePath	FilePath
FileName	FileName
MD5	FileHash
FileSize	FileSize

3. Для событий, перечисленными в таблице ниже, должна быть настроена дополнительная нормализация с копированием полей в соответствии с таблицей.

   Дополнительная нормализация с копированием полей событий из KATA/EDR

Событие	Поле сырого события	Поле нормализованного события
Процесс	UniqueParentPid	FlexString1
	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
AppLock	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
BlockedDocument	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName

Событие	Поле сырого события	Поле нормализованного события
Module	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
FileChange	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
Driver	HostName	DeviceHostName
	FileName	FileName
	ProductName	DeviceCustomString5
		ProductName
	ProductVendor	DeviceCustomString6
		ProductVendor
Connection	UniquePid	FlexString2
	HostName	DeviceHostName
	URI	RequestURL
	RemoteIP	DestinationAddress
	RemotePort	DestinationPort
PortListen	UniquePid	FlexString2
	HostName	DeviceHostName
	LocalIP	SourceAddress
	LocalPort	SourcePort
Registry	UniquePid	FlexString2
	HostName	DeviceHostName
	ValueName	DeviceCustomString5
		New Value Name
	KeyName	DeviceCustomString4
		New Key Name
	PreviousKeyName	FlexString2
		Old Key Name
	ValueData	DeviceCustomString6
		New Value Data
	PreviousValueData	FlexString1
		Old Value Data
	ValueType	FlexNumber1
		Value Type
	PreviousValueType	FlexNumber2
		Previous Value Type

Событие	Поле сырого события	Поле нормализованного события
SystemEventLog	UniquePid	FlexString2
	HostName	DeviceHostName
	OperationResult	EventOutcome
	EventId	DeviceCustomNumber3
		EventId
	EventRecordId	DeviceCustomNumber2
		EventRecordId
	Channel	DeviceCustomString6
		Channel
	ProviderName	SourceUserID
ThreatDetect	UniquePid	FlexString2
	HostName	DeviceHostName
	VerdictName	EventOutcome
	DetectedObjectType	OldFileType
	isSilent	FlexString1
		Is Silent
	RecordId	DeviceCustomString5
		Record ID
	DatabaseTimestamp	DeviceCustomDate2
		Database Timestamp
ThreatDetectProcessingResult	UniquePid	FlexString2
	HostName	DeviceHostName
	ThreatStatus	DeviceCustomString5
		Threat Status
PROCESS_INTERPRET_FILE_RUN	UniquePid	FlexString2
	HostName	DeviceHostName
	FileName	FileName
	InterpretedFilePath	OldFilePath
	InterpretedFileSize	OldFileSize
	InterpretedFileHash	OldFileHash
PROCESS_CONSOLE_INTERACTIVE_INPUT	UniquePid	FlexString2
	HostName	DeviceHostName
	InteractiveInputText	DeviceCustomString4
		Command Line
AMSI SCAN	UniquePid	FlexString2
	HostName	DeviceHostName
	ObjectContent	DeviceCustomString5
		Object Content

Модель данных актива

Структура актива представлена полями, в которых содержатся значения. Поля также могут содержать вложенные структуры.

Поле актива	Тип значения	Описание
`ID`	Строка	Идентификатор актива.
`TenantName`	Строка	Название тенанта.
`DeletedAt`	Число	Дата удаления актива.
`CreatedAt`	Число	Дата создания актива.
`TenantID`	Строка	Идентификатор тенанта.
`DirectCategories`	Вложенный список строк	Категории актива.
`CategoryModels`	Вложенная структура `[Category]`	Изменение категорий актива.
`AffectedByIncidents`	Вложенный словарь: [строка:строка `TRUE/FALSE`]	Идентификаторы инцидентов.
`IPAddress`	Вложенный список строк	IP-адреса актива.
`FQDN`	Строка	FQDN актива.
`Weight`	Число	Уровень важности актива.
`Deleted`	Строка со значениями `TRUE/FALSE`	Помечен ли актив на удаление из KUMA.
`UpdatedAt`	Число	Дата последнего обновления актива.
`MACAddress`	Вложенный список строк	MAC-адреса актива.
`IPAddressInt`	Вложенный список чисел	IP-адрес в виде числа.
`Owner`	Вложенная структура [OwnerInfo]	Сведения о владельце актива.
`OS`	Вложенная структура [OS]	Сведения об операционной системы актива.
`DisplayName`	Строка	Название актива.
`APISoft`	Вложенная структура [Software]	ПО, установленное на активе.
`APIVulns`	Вложенная структура [Vulnerability]	Уязвимости актива.
`KICSServerIp`	Строка	IP-адрес сервера KICS for Networks.
`KICSConnectorID`	Число	Идентификатор коннектора KICS for Networks.
`KICSDeviceID`	Число	Идентификатор актива в KICS for Networks.
`KICSStatus`	Строка	Статус актива в KICS for Networks.
`KICSHardware`	Вложенная структура [KICSSystemInfo]	Аппаратные сведения об активе, полученные из KICS for Networks.
`KICSSoft`	Вложенная структура [KICSSystemInfo]	Сведения о ПО актива, полученные из KICS for Networks.
`KICSRisks`	Вложенная структура [KICSRisk]	Сведения об уязвимостях актива, полученные из KICS for Networks.
`Sources`	Вложенная структура [Sources]	Основные сведения об активе, поступавшие из разных источников.
`FromKSC`	Строка со значениями `TRUE/FALSE`	Индикатор, указывающий, что сведения об активе импортированы из Kaspersky Security Center.

NAgentID	Строка	Идентификатор Агента администрирования Kaspersky Security Center, от которого получены сведения об активе.
KSCServerFQDN	Строка	FQDN Сервера Kaspersky Security Center.
KSCInstanceID	Строка	Идентификатор экземпляра Kaspersky Security Center.
KSCMasterHostname	Строка	Имя устройства Сервера администрирования Kaspersky Security Center.
KSCGroupID	Число	Идентификатор группы Kaspersky Security Center.
KSCGroupName	Строка	Название группы администрирования Kaspersky Security Center.
LastVisible	Число	Дата, когда от Kaspersky Security Center в последний раз были получены сведения об активе.
Products	Вложенный словарь: [строка:вложенная структура [ProductInfo]	Сведения об установленных на активе приложениях Kaspersky, полученные из Kaspersky Security Center.
Hardware	Вложенная структура [Hardware]	Аппаратные сведения об активе, полученные из Kaspersky Security Center.
KSCSoft	Вложенная структура [Software]	Сведения о ПО актива, полученные из Kaspersky Security Center.
KSCVulns	Вложенная структура [Vulnerability]	Сведения об уязвимостях актива, полученные из Kaspersky Security Center.

Вложенная структура Category

Поле	Тип значения	Описание
ID	Строка	Идентификатор категории.
TenantID	Строка	Идентификатор тенанта.
TenantName	Строка	Название тенанта.
Parent	Строка	Родительская категория.
Path	Вложенный список строк	Структура категорий.
Имя	Строка	Название категории.
UpdatedAt	Число	Последнее обновление категории.
CreatedAt	Число	Дата создания категории.
Описание	Строка	Описание категории.
Weight	Число	Уровень важности категории.
CategorizationKind	Строка	Тип присвоения категории активам.
CategorizationAt	Число	Дата категоризации.
CategorizationInterval	Строка	Интервал присвоения категорий.

Вложенная структура OwnerInfo

Поле	Тип значения	Описание
DisplayName	Строка	Имя владельца актива.

Вложенная структура OS

Поле	Тип значения	Описание
`Имя`	Строка	Название операционной системы.
`BuildNumber`	Число	Версия операционной системы.

Вложенная структура Software

Поле	Тип значения	Описание
`DisplayName`	Строка	Название ПО.
`DisplayVersion`	Строка	Версия ПО.
`Publisher`	Строка	Издатель ПО.
`InstallDate`	Строка	Дата установки.
`HasMSIInstaller`	Строка `TRUE/FALSE`	Признак, имеет ли ПО MSI-установщик.

Вложенная структура Vulnerability

Поле	Тип значения	Описание
`KasperskyID`	Строка	Идентификатор уязвимости, присвоенный Kaspersky.
`ProductName`	Строка	Название ПО.
`DescriptionURL`	Строка	URL с описанием уязвимости.
`RecommendedMajorPatch`	Строка	Рекомендуемое обновление.
`RecommendedMinorPatch`	Строка	Рекомендуемое обновление.
`SeverityStr`	Строка	Уровень важности уязвимости.
`Severity`	Число	Уровень важности уязвимости.
`CVE`	Вложенный список строк	Идентификатор уязвимости CVE.
`ExploitExists`	Строка `TRUE/FALSE`	Существует ли эксплойт.
`MalwareExists`	Строка `TRUE/FALSE`	Существует ли вредоносное приложение.

Вложенная структура KICSSystemInfo

Поле	Тип значения	Описание
`Model`	Строка	Модель устройства.
`Версия`	Строка	Версия устройства.
`Производитель;`	Строка	Производитель.

Вложенная структура KICSRisk

Поле	Тип значения	Описание
`ID`	Число	Идентификатор риска KICS for Networks.
`Имя`	Строка	Название риска.
`Category`	Строка	Тип риска.
`Описание`	Строка	Описание риска.
`DescriptionUrl`	Строка	Ссылка на описание риска.
`Severity`	Число	Уровень важности риска.
`Cvss`	Число	Оценка CVSS.

Вложенная структура Sources

Поле	Тип значения	Описание
`KSC`	Вложенная структура [SourceInfo]	Сведения об активе, полученные из Kaspersky Security Center.
`API`	Вложенная структура [SourceInfo]	Сведения об активе, поступившие через REST API.
`Manual`	Вложенная структура [SourceInfo]	Сведения об активе, введенные вручную.
`KICS`	Вложенная структура [SourceInfo]	Сведения об активе, поступившие из KICS for Networks.

Вложенная структура Sources

Поле	Тип значения	Описание
`MACAddress`	Вложенный список строк	MAC-адреса актива.
`IPAddressInt`	Вложенный список чисел	IP-адрес в виде числа.
`Owner`	Вложенная структура [OwnerInfo]	Сведения о владельце актива.
`OS`	Вложенная структура [OS]	Сведения об операционной системы актива.
`DisplayName`	Строка	Название актива.
`IPAddress`	Вложенный список строк	IP-адреса актива.
`FQDN`	Строка	FQDN актива.
`Weight`	Число	Уровень важности актива.
`Deleted`	Строка со значениями `TRUE/FALSE`	Помечен ли актив на удаление из KUMA.
`UpdatedAt`	Число	Дата последнего обновления актива.

Вложенная структура ProductInfo

Поле	Тип значения	Описание
`ProductVersion`	Строка	Версия ПО.
`ProductName`	Строка	Название ПО.

Вложенная структура Hardware

Поле	Тип значения	Описание
`NetCards`	Вложенная структура [NetCard]	Перечень сетевых карт актива.
`Процессор`	Вложенная структура [CPU]	Перечень процессоров актива.
`ОЗУ`	Вложенная структура [RAM]	Перечень ОЗУ актива.
`Disk`	Вложенная структура [Disk]	Перечень дисков актива.

Вложенная структура NetCard

Поле	Тип значения	Описание
`ID`	Строка	Идентификатор сетевой карты.
`MACAddresses`	Вложенный список строк	MAC-адреса сетевой карты.
`Имя`	Строка	Название сетевой карты.
`Manufacture`	Строка	Производитель сетевой карты.
`DriverVersion`	Строка	Версия драйвера.

Вложенная структура RAM

Поле	Тип значения	Описание
`Frequency`	Строка	Частота ОЗУ.
`TotalBytes`	Число	Объем ОЗУ в байтах.

Вложенная структура CPU

Поле	Тип значения	Описание
`ID`	Строка	Идентификатор процессора.
`Имя`	Строка	Название процессора.

`CoreCount`	Строка	Количество ядер.
`CoreSpeed`	Строка	Частота.

Вложенная структура Disk

Поле	Тип значения	Описание
`FreeBytes`	Число	Свободное пространство на диске.
`TotalBytes`	Число	Общее пространство на диске.

Модель данных учетной записи

К полям учетной записи можно обращаться из шаблонов электронной почты, а также при корреляции событий.

Поле	Тип значения	Описание
`ID`	Строка	Идентификатор учетной записи.
`ObjectGUID`	Строка	Атрибут Active Directory. Идентификатор учетной записи в Active Directory.
`TenantID`	Строка	Идентификатор тенанта.
`TenantName`	Строка	Название тенанта.
`UpdatedAt`	Число	Последнее обновление учетной записи.
`Domain`	Строка	Домен.
`CN`	Строка	Атрибут Active Directory. Имя пользователя.
`DisplayName`	Строка	Атрибут Active Directory. Отображаемое имя пользователя.
`DistinguishedName`	Строка	Атрибут Active Directory. Название объекта LDAP.
`EmployeeID`	Строка	Атрибут Active Directory. Идентификатор сотрудника.
`Mail`	Строка	Атрибут Active Directory. Электронная почта пользователя.
`MailNickname`	Строка	Атрибут Active Directory. Альтернативный адрес электронной почты.
`Mobile`	Строка	Атрибут Active Directory. Номер мобильного телефона.
`ObjectSID`	Строка	Атрибут Active Directory. Идентификатор безопасности.
`SAMAccountName`	Строка	Атрибут Active Directory. Учетная запись.
`TelephoneNumber`	Строка	Атрибут Active Directory. Номер телефона.
`UserPrincipalName`	Строка	Атрибут Active Directory. Имя участника-пользователя.
`Archived`	`Строка TRUE/FALSE`	Признак, определяющий, является ли учетная запись устаревшей.
`MemberOf`	Список строк	Атрибут Active Directory. Группы Active Directory, в которые внесен пользователь. По этому атрибуту события можно искать при корреляции.
`PreliminarilyArchived`	`Строка TRUE/FALSE`	Признак, определяющий, требуется ли обозначить учетную запись как устаревшую.
`CreatedAt`	Число	Дата создания учетной записи.
`SN`	Строка	Атрибут Active Directory. Фамилия пользователя.

SAMAccountType	Строка	Атрибут Active Directory. Тип учетной записи.
Title	Строка	Атрибут Active Directory. Должность пользователя.
Division	Строка	Атрибут Active Directory. Подразделение пользователя.
Department	Строка	Атрибут Active Directory. Отдел пользователя.
Manager	Строка	Атрибут Active Directory. Руководитель пользователя.
Расположение	Строка	Атрибут Active Directory. Местоположение пользователя.
Company	Строка	Атрибут Active Directory. Компания пользователя.
StreetAddress	Строка	Атрибут Active Directory. Адрес компании.
PhysicalDeliveryOfficeName	Строка	Атрибут Active Directory. Адрес для доставки.
ManagedObjects	Список строк	Атрибут Active Directory. Объекты, находящиеся под управлением пользователя.
UserAccountControl	Число	Атрибут Active Directory. Тип учетной записи Active Directory.
WhenCreated	Число	Атрибут Active Directory. Дата создания учетной записи.
WhenChanged	Число	Атрибут Active Directory. Дата изменения учетной записи.
AccountExpires	Число	Атрибут Active Directory. Дата истечения срока учетной записи.
BadPasswordTime	Число	Атрибут Active Directory. Дата последней неудачной попытки входа в систему.

Порты, используемые Kaspersky SIEM Cloud

Для правильной работы программы нужно убедиться, что компоненты Kaspersky SIEM Cloud могут взаимодействовать с другими компонентами и программами по сети.

Маршрутизация подключений к Ядру Kaspersky SIEM Cloud и сервисам Kaspersky SIEM Cloud выполняется по имени хоста в TLS-рукопожатии. Между инфраструктурой организации и облачной инфраструктурой не должно быть прокси-серверов и межсетевых экранов, которые перехватывают и подменяют TLS-соединения.

Порты для компонентов Kaspersky SIEM Cloud

В таблице ниже показаны значения сетевых портов, используемых компонентами Kaspersky SIEM Cloud.

Сетевые порты, используемые для взаимодействия компонентов Kaspersky SIEM Cloud

Протокол	Порт	Направление	Назначение подключения
HTTPS	443	От браузера пользователя к OSMP Console.	Доступ пользователей к веб-интерфейсу Kaspersky SIEM Cloud в составе OSMP Console.
HTTPS	443	От инфраструктуры организации к публичному API OSMP.	Вызовы API Kaspersky SIEM Cloud.
TCP (TLS)	443	От локального коллектора к Ядру Kaspersky SIEM Cloud в облачной инфраструктуре.	Соединение локального коллектора с Ядром Kaspersky SIEM Cloud, получение конфигурации, управляющее WebSocket-соединение (получение статуса, журналов, метрик, перезапуск сервиса, перезагрузка конфигурации). Соединение постоянное, инициируется коллектором.

TCP (TLS)	443	От локального коллектора к сервисам в облачной инфраструктуре, указанным в его точках назначения: хранилищу, коррелятору или маршрутизатору событий.	Передача нормализованных событий в облачную инфраструктуру.
TCP (TLS)	443	От источников событий (например, от Kaspersky Endpoint Security или агентов Kaspersky SIEM Cloud) к облачному коллектору.	Передача телеметрии в облачный коллектор.

Порты, используемые на хосте локального коллектора

Коллектор, установленный в локальной инфраструктуре организации, использует следующие порты:

- TCP и UDP порты коннекторов коллектора, указанные при создании ресурса коллектора.

  Направление: от источников событий к коллектору.

  Назначение: прием событий.

  Если вы используете предустановленный коллектор из состава OOTB, по умолчанию используются порты:

  - 7230/tcp
  - 7231/tcp
  - 7232/tcp
  - 7233/tcp
  - 7234/tcp
  - 7235/tcp
  - 5140/tcp
  - 5140/udp
  - 5141/tcp
  - 5144/udp

- TCP порт 7221 или другой порт, заданный параметром `--api.port` при установке коллектора.

  Направление: локальные обращения на хосте коллектора. Открывать порт для подключений извне не требуется.

  Назначение: служебный API коллектора, используемый для проверки работоспособности коллектора и выгрузки файлов дампа.

События аудита Kaspersky SIEM Cloud

События аудита создаются при выполнении в Kaspersky SIEM Cloud определенных действий, связанных с безопасностью, и используются для обеспечения целостности системы.

События аудита создаются на сервере Ядра Kaspersky SIEM Cloud и отправляются в хранилища тенанта Main и корреляторы тенанта Main. Поэтому для хранения событий аудита должно быть создано хотя бы одно хранилище в тенанте Main. Если хранилища нет, вам нужно создать его. События аудита отправляются в пространство KUMA Audit, которое создается автоматически внутри хранилища.

Чтобы просмотреть события аудита, вам нужно перейти в раздел Kaspersky SIEM Cloud **События** и добавить в запрос `SELECT * FROM 'events' WHERE Type=4`.

В результате выполнения запроса отобразятся события аудита, если роль пользователя предусматривает права для просмотра событий аудита.

Поля событий с общей информацией

Каждое событие аудита имеет поля событий, описанные в таблице ниже.

Название поля события	Значение поля
`Timestamp`	Время события.
`DeviceHostName`	Хост источника события. Для событий аудита указывается имя хоста, на котором установлена служба kuma-core, потому что она является источником событий.
`DeviceTimeZone`	Часовой пояс системного времени сервера, на котором установлено Ядро Kaspersky SIEM Cloud в формате `+-чч:мм`.
`Type`	Тип события аудита. `Audit` или `Base`.
`TenantID`	Идентификатор тенанта.
`DeviceVendor`	`Kaspersky`
`DeviceProduct`	`KUMA`
`EndTime`	Время создания события.
`SpaceID`	`KUMA Audit`
`DeviceAction`	Действие, которое зафиксировано в событии аудита.

Пользователь изменил параметры набора полей для определения источников

Название поля события	Значение поля
`DeviceAction`	`settings updated`
`DeviceFacility`	`eventSourceIdentity`
`EventOutcome`	`succeeded`
`SourceUserName`	Логин пользователя, который внес изменения.
`SourceUserID`	Идентификатор пользователя, который внес изменения.
`DeviceCustomString5`	Обновленный набор полей, | используется в качестве разделителя.

Добавлен файл ключа

Название поля события	Значение поля
DeviceAction	license key installed
EventOutcome	succeeded
Message	Название лицензии.
SourceUserID	Идентификатор пользователя, который добавил файл ключа.
SourceUserName	Логин пользователя, который добавил файл ключа.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Резервный лицензионный ключ добавлен

Название поля события	Значение поля
DeviceAction	reserve license key installed
DeviceAddress	IP-адрес устройства, на котором добавлен резервный лицензионный ключ.
EventOutcome	succeeded
Message	Название лицензии.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserID	Идентификатор пользователя, который добавил резервный лицензионный ключ.
SourceUserName	Логин пользователя, который добавил резервный лицензионный ключ.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Резервный лицензионный ключ удален

Название поля события	Значение поля
DeviceAction	reserve license key uninstalled
DeviceAddress	IP-адрес устройства, на котором удален резервный лицензионный ключ.

EventOutcome	succeeded
Message	Название лицензии.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserID	Идентификатор пользователя, который удалил резервный лицензионный ключ.
SourceUserName	Логин пользователя, который удалил резервный лицензионный ключ.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Приложение активировано с помощью кода активации

Название поля события	Значение поля
DeviceAction	license activated
EventOutcome	succeeded
Message	Название лицензии.
SourceUserID	Идентификатор пользователя, который указал код активации.
SourceUserName	Логин пользователя, который указал код активации.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Срок действия лицензии продлен

Название поля события	Значение поля
DeviceAction	license reactivated
EventOutcome	succeeded
Message	Название лицензии.
SourceUserID	Идентификатор пользователя, который добавил файл ключа.
SourceUserName	Логин пользователя, который добавил файл ключа.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.

SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Недействительный код активации

Название поля события	Значение поля
DeviceAction	activation code license activated
EventOutcome	failed
Message	Текст ошибки.
SourceUserID	Идентификатор пользователя, который указал код активации.
SourceUserName	Логин пользователя, который указал код активации.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Код активации заблокирован

Название поля события	Значение поля
DeviceAction	Activation code blocked
EventOutcome	succeeded
Message	Название лицензии.
SourceUserID	Идентификатор пользователя, который указал код активации.
SourceUserName	Логин пользователя, который указал код активации.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Код активации или файл ключа удален

Название поля события	Значение поля
DeviceAction	Activation code or key file uninstalled
EventOutcome	succeeded
Message	Название лицензии.
SourceUserID	Идентификатор пользователя, который удалил файл ключа.

SourceUserName	Логин пользователя, который удалил файл ключа.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Превышено количество EPS

Название поля события	Значение поля
DeviceAction	`license limit for EPS exceeded`
EventOutcome	`succeeded`
Message	Название лицензии.
SourceUserID	Идентификатор пользователя, который добавил файл ключа или указал код активации.
SourceUserName	Логин пользователя, который добавил файл ключа или указал код активации.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Окончание срока действия лицензии и начало льготного периода

Название поля события	Значение поля
DeviceAction	`license expired`
EventOutcome	`succeeded`
Message	Название лицензии.
SourceUserID	Идентификатор пользователя, который добавил файл ключа или указал код активации.
SourceUserName	Логин пользователя, который добавил файл ключа или указал код активации.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Окончание льготного периода

Название поля события	Значение поля
DeviceAction	license ended
EventOutcome	succeeded
Message	Название лицензии.
SourceUserID	Идентификатор пользователя, который добавил файл ключа или указал код активации.
SourceUserName	Логин пользователя, который добавил файл ключа или указал код активации.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

Добавлен код активации или файл ключа с истекшим сроком годности

Название поля события	Значение поля
DeviceAction	Activation code or key file installed
IP	IP-адрес, на котором добавлен файл ключа или указан код активации.
EventOutcome	failed
Message	Текст ошибки.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserID	Идентификатор пользователя, который добавил файл ключа или указал код активации.
SourceUserName	Логин пользователя, который добавил файл ключа или указал код активации.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Изменен набор пространств для разграничения доступа к событиям

Название поля события	Значение поля
DeviceAction	• space set was created • space set was deleted • space set was updated (включая выдачу прав доступа и отзыв прав доступа)
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который изменил параметры.
SourceUserID	Идентификатор пользователя, который изменил параметры.
DeviceCustomString5	Идентификатор набора пространств.
DeviceCustomString5Label	set ID
DeviceCustomString3	Название набора пространств.
DeviceCustomString3Label	space name

Изменены пороговые значения для мониторинга сервисов

Название поля события	Значение поля
DeviceAction	settings updated
DeviceFacility	serviceAlertSettings
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который изменил параметры.
SourceUserID	Идентификатор пользователя, который изменил параметры.
DeviceCustomString1	JSON с пороговыми значениями, записанными в базе данных.
DeviceCustomString1Label	thresholds
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Изменены значения параметров Ядра Kaspersky SIEM Cloud

Название поля события	Значение поля
DeviceAction	settings updated
DeviceFacility	coreProperties
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который изменил параметры.
SourceUserID	Идентификатор пользователя, который изменил параметры.
DeviceCustomString1	JSON со значениями параметров Ядра Kaspersky SIEM Cloud, записанными в базе данных.
DeviceCustomString1Label	properties

Базы GeoIP импортированы

Название поля события	Значение поля
DeviceAction	new geobase imported
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который импортировал базы.
SourceUserID	Идентификатор пользователя, который импортировал базы.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Сервис создан

Название поля события	Значение поля
DeviceAction	service created
EventOutcome	succeeded

SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который создал сервис.
SourceUserID	Идентификатор пользователя, который создал сервис.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Сервис удален

Название поля события	Значение поля
DeviceAction	service deleted
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который удалил сервис.
SourceUserID	Идентификатор пользователя, который удалил сервис.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DestinationAddress	Адрес устройства, с которого был запущен сервис. Если сервис никогда раньше не запускался, поле будет пустым.
DestinationHostName	Полное доменное имя компьютера, с которого был запущен сервис. Если сервис никогда раньше не запускался, поле будет пустым.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Сервис перезагружен

Название поля события	Значение поля
DeviceAction	service reloaded
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который перезагрузил сервис.
SourceUserID	Идентификатор пользователя, который перезагрузил сервис.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Сервис перезапущен

Название поля события	Значение поля
DeviceAction	service restarted
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который перезапустил сервис.
SourceUserID	Идентификатор пользователя, который перезапустил сервис.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Сервис запущен

Название поля события	Значение поля
DeviceAction	service started
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DestinationAddress	Адрес устройства, на котором был запущен сервис.
DestinationHostName	Полное доменное имя устройства, на котором был запущен сервис.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Сервис сопряжен

Название поля события	Значение поля
DeviceAction	service paired
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Статус сервиса изменен

Название поля события	Значение поля
DeviceAction	service status changed
DeviceExternalID	Идентификатор сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DestinationAddress	Адрес устройства, на котором был запущен сервис.
DestinationHostName	Полное доменное имя устройства, на котором был запущен сервис.
DeviceCustomString1	green, yellow или red
DeviceCustomString1Label	new status
DeviceCustomString2	green, yellow или red
DeviceCustomString2Label	old status
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Партиция удалена пользователем

Название поля события	Значение поля
DeviceAction	partition deleted
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который удалил партицию.
SourceUserID	Идентификатор пользователя, который удалил партицию.
Name	Название хранилища | Тенант перемещаемой или удаляемой партиции | Название пространства, которому принадлежит партиция.
DeviceCustomDate1	Время изменения данных в формате UTC. Дата, которая отображается в партициях хранилища в столбце date.
DeviceCustomDate1Label	date of event
Message	deleted by user

Партиция удалена автоматически по истечении срока хранения

Название поля события	Значение поля
DeviceAction	partition deleted
EventOutcome	succeeded
Name	Название пространства, которому принадлежит партиция.
DeviceCustomDate1	Время изменения данных в формате UTC. Дата, которая отображается в партициях хранилища в столбце date.
DeviceCustomDate1Label	date of event
SourceServiceName	scheduler
Message	deleted by retention period settings

Удаление партиции по абсолютному сроку хранения

Название поля события	Значение поля
Name	Название пространства, которому принадлежит партиция.
Message	deleted partition data
DeviceAction	applied retention policy by GB
SourceServiceName	scheduler
DeviceCustomDate1	Время изменения данных в формате UTC. Дата, которая отображается в партициях хранилища в столбце date.
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	Размер партиции.
DeviceCustomNumber1Label	size
DeviceCustomNumber2	Количество событий.
DeviceCustomNumber2Label	events
EventOutcome	succeeded

Удаление партиции по относительному сроку хранения

Название поля события	Значение поля
Name	Название пространства, которому принадлежит партиция.
Message	deleted partition data
DeviceAction	applied retention policy by percent
SourceServiceName	scheduler
DeviceCustomDate1	Время изменения данных в формате UTC. Дата, которая отображается в партициях хранилища в столбце date.
DeviceCustomDate1Label	date of partition

DeviceCustomNumber1	Размер партиции.
DeviceCustomNumber1Label	size
DeviceCustomNumber2	Количество событий.
DeviceCustomNumber2Label	events
EventOutcome	succeeded

Перемещение партиции в холодное хранилище

Название поля события	Значение поля
Name	Название пространства, которому принадлежит партиция.
Message	moved partition data to cold storage
DeviceAction	Доступны следующие значения: • applied retention policy by days • applied retention policy by percent • applied retention policy by GB
SourceServiceName	scheduler
DeviceCustomDate1	Время изменения данных в формате UTC. Дата, которая отображается в партициях хранилища в столбце date.
DeviceCustomDate1Label	date of partition
DeviceCustomNumber1	Размер партиции.
DeviceCustomNumber1Label	size
DeviceCustomNumber2	Количество событий.
DeviceCustomNumber2Label	events
EventOutcome	succeeded
DeviceCustomString1	Идентификатор пространства.
DeviceCustomString1Label	nodeID

Перемещение партиции в холодное хранилище завершилось с ошибкой

Название поля события	Значение поля
Name	Название пространства, которому принадлежит партиция.
Message	move partition data to cold storage failed: {"error":"Code: 243. DB::Exception: Move is not possible. Not enough space on 'cold_volume'. (NOT_ENOUGH_SPACE) (version 23.8.8.207)\n"}
DeviceAction	Доступны следующие значения: • applied retention policy by days • applied retention policy by percent • applied retention policy by GB
SourceServiceName	scheduler
DeviceCustomDate1	Время изменения данных в формате UTC. Дата, которая отображается в партициях хранилища в столбце date.
DeviceCustomDate1Label	date of partition

DeviceCustomNumber1	Размер партиции.
DeviceCustomNumber1Label	size
DeviceCustomNumber2	Количество событий.
DeviceCustomNumber2Label	events
EventOutcome	failed
DeviceCustomString1	Идентификатор пространства.
DeviceCustomString1Label	nodeID

Активный лист успешно очищен или операция завершилась с ошибкой

События аудита по активным листам создаются только для действий, совершенных пользователями. При изменении активных листов с помощью правил корреляции события аудита не создаются. **Если необходимо отслеживать такие изменения, это можно сделать с помощью алертов**.

Если изменять активный лист с помощью правила корреляции типа **simple**, в котором заданы действия **Отправить событие на дальнейшую обработку** и **Отправить событие снова в коррелятор**, то в результате срабатывания такого правила будет создаваться алерт об изменении активного листа.

Событию может быть присвоен статус `succeeded` или `failed`.

Поскольку запрос на очистку активного листа осуществляется через удаленное соединение, ошибка передачи данных может возникнуть в любой момент: до удаления или после удаления.

Это означает, что активный лист может быть очищен успешно, но событие все равно будет иметь статус `failed`, поскольку EventOutcome возвращает статус TCP/IP-соединения запроса, а не статус проверки, был ли очищен активный лист.

Значения полей события аудита Активный лист успешно очищен или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	active list cleared
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для очистки активного листа.
SourceUserID	Идентификатор пользователя, который использовался для очистки активного листа.
DeviceExternalID	Идентификатор сервиса, активные лист которого был очищен.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID

DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Элемент активного листа успешно изменен или операция завершилась с ошибкой

События аудита по активным листам создаются только для действий, совершенных пользователями. При изменении активных листов с помощью правил корреляции события аудита не создаются. **Если необходимо отслеживать такие изменения, это можно сделать с помощью алертов**.

Если изменять активный лист с помощью правила корреляции типа **simple**, в котором заданы действия **Отправить событие на дальнейшую обработку** и **Отправить событие снова в коррелятор**, то в результате срабатывания такого правила будет создаваться алерт об изменении активного листа.

Событию может быть присвоен статус `succeeded` или `failed`.

Поскольку запрос на изменение элемента активного листа осуществляется через удаленное соединение, ошибка передачи данных может возникнуть в любой момент: до изменения или после изменения.

Это означает, что элемент активного листа может быть изменен успешно, но событие все равно будет иметь статус `failed`, поскольку EventOutcome возвращает статус TCP/IP-соединения запроса, а не статус проверки, был ли изменен элемент активного листа.

Значения полей события аудита Элемент активного листа успешно изменен или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	`active list item changed`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для изменения элемента активного листа.
SourceUserID	Идентификатор пользователя, который использовался для изменения элемента активного листа.
DeviceExternalID	Идентификатор сервиса, активный лист которого был изменен.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
DeviceCustomString1	Название ключа.
DeviceCustomString1Label	`key`
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	название тенанта
DeviceCustomString6Label	`tenant name`

Элемент активного листа успешно удален или операция завершилась с ошибкой

События аудита по активным листам создаются только для действий, совершенных пользователями. При изменении активных листов с помощью правил корреляции события аудита не создаются. **Если необходимо отслеживать такие изменения, это можно сделать с помощью алертов**.

Если изменять активный лист с помощью правила корреляции типа **simple**, в котором заданы действия **Отправить событие на дальнейшую обработку** и **Отправить событие снова в коррелятор**, то в результате срабатывания такого правила будет создаваться алерт об изменении активного листа.

Событию может быть присвоен статус `succeeded` или `failed`.

Поскольку запрос на удаление элемента активного листа осуществляется через удаленное соединение, ошибка передачи данных может возникнуть в любой момент: до удаления или после удаления.

Это означает, что элемент активного листа может быть удален успешно, но событие все равно будет иметь статус `failed`, поскольку EventOutcome возвращает статус TCP/IP-соединения запроса, а не статус проверки, был ли удален элемент активного листа.

Значения полей события аудита Элемент активного листа успешно удален или операция завершилась с ошибкой

Название поля события	Значение поля
`DeviceAction`	`active list item deleted`
`EventOutcome`	`succeeded` или `failed`
`SourceTranslatedAddress`	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
`SourceAddress`	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
`SourcePort`	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
`SourceUserName`	Логин пользователя, который использовался для удаления элемента активного листа.
`SourceUserID`	Идентификатор пользователя, который использовался для удаления элемента активного листа.
`DeviceExternalID`	Идентификатор сервиса, активный лист которого был очищен.
`ExternalID`	Идентификатор активного листа.
`Name`	Название активного листа.
`DeviceCustomString1`	Название ключа.
`DeviceCustomString1Label`	`key`
`Message`	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.
`DeviceCustomString5`	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
`DeviceCustomString5Label`	`tenant ID`
`DeviceCustomString6`	Название тенанта.
`DeviceCustomString6Label`	`tenant name`

Активный лист успешно импортирован или операция завершилась с ошибкой

События аудита по активным листам создаются только для действий, совершенных пользователями. При изменении активных листов с помощью правил корреляции события аудита не создаются. **Если необходимо отслеживать такие изменения, это можно сделать с помощью алертов**.

Если изменять активный лист с помощью правила корреляции типа **simple**, в котором заданы действия **Отправить событие на дальнейшую обработку** и **Отправить событие снова в коррелятор**, то в результате срабатывания такого правила будет создаваться алерт об изменении активного листа.

Импорт элементов активного листа выполняется по частям через удаленное подключение.

Поскольку импорт осуществляется через удаленное соединение, ошибка передачи данных может произойти в любой момент: когда данные частично или полностью импортированы. EventOutcome возвращает статус подключения, а не статус проверки импорта.

Значения полей события аудита Активный лист успешно импортирован или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	active list imported
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для выполнения импорта.
SourceUserID	Идентификатор пользователя, который использовался для импорта.
DeviceExternalID	Идентификатор сервиса, для которого был выполнен импорт.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке. Текст ошибки может быть в формате json, например {"error":"line 1: header does not contain column IP!"}.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	название тенанта
DeviceCustomString6Label	tenant name

Активный лист экспортирован

События аудита по активным листам создаются только для действий, совершенных пользователями. При изменении активных листов с помощью правил корреляции события аудита не создаются. **Если необходимо отслеживать такие изменения, это можно сделать с помощью алертов**.

Если изменять активный лист с помощью правила корреляции типа **simple**, в котором заданы действия **Отправить событие на дальнейшую обработку** и **Отправить событие снова в коррелятор**, то в результате срабатывания такого правила будет создаваться алерт об изменении активного листа.

Значения полей события аудита Активный лист экспортирован

Название поля события	Значение поля
DeviceAction	active list exported
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для выполнения экспорта.
SourceUserID	Идентификатор пользователя, который использовался для экспорта.
DeviceExternalID	Идентификатор сервиса, для которого был выполнен экспорт.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	название тенанта
DeviceCustomString6Label	tenant name

Контекстная таблица экспортирована

События аудита по контекстным таблицам создаются только для действий, совершенных пользователями.

Значения полей события аудита Контекстная таблица экспортирована

Название поля события	Значение поля
DeviceAction	context table exported
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для выполнения экспорта.
SourceUserID	Идентификатор пользователя, который использовался для экспорта.
DeviceExternalID	Идентификатор сервиса, для которого был выполнен экспорт.
ExternalID	Идентификатор контекстной таблицы.
Name	Название контекстной таблицы.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID

DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Контекстная таблица успешно импортирована или операция завершилась с ошибкой

События аудита по контекстным таблицам создаются только для действий, совершенных пользователями.

Импорт элементов контекстной таблицы выполняется по частям через удаленное подключение.

Поскольку импорт осуществляется через удаленное соединение, ошибка передачи данных может произойти в любой момент: когда данные частично или полностью импортированы. EventOutcome возвращает статус подключения, а не статус проверки импорта.

Значения полей события аудита Контекстная таблица успешно импортирована или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	context table imported
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для выполнения импорта.
SourceUserID	Идентификатор пользователя, который использовался для импорта.
DeviceExternalID	Идентификатор сервиса, для которого был выполнен импорт.
ExternalID	Идентификатор контекстной таблицы.
Name	Название контекстной таблицы.
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Элемент контекстной таблицы успешно изменен или операция завершилась с ошибкой

События аудита по контекстным таблицам создаются только для действий, совершенных пользователями.

Событию может быть присвоен статус succeeded или failed.

Параметры события аудита Элемент контекстной таблицы успешно изменен или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	context table item is set
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для изменения элемента контекстной таблицы.
SourceUserID	Идентификатор пользователя, который использовался для изменения элемента контекстной таблицы.
DeviceExternalID	Идентификатор сервиса, контекстная таблица которого была изменена.
ExternalID	Идентификатор контекстной таблицы.
Name	Название контекстной таблицы.
DeviceCustomString1	Название ключа записи.
DeviceCustomString1Label	key
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Элемент контекстной таблицы успешно удален или операция завершилась с ошибкой

События аудита по контекстным таблицам создаются только для действий, совершенных пользователями.

Событию может быть присвоен статус succeeded или failed.

Значения полей события аудита Элемент контекстной таблицы успешно удален или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	context table item deleted
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для удаления элемента контекстной таблицы.
SourceUserID	Идентификатор пользователя, который использовался для удаления элемента контекстной таблицы.
DeviceExternalID	Идентификатор сервиса, для которого происходит удаление элемента контекстной таблицы.
ExternalID	Идентификатор контекстной таблицы.

Name	Название контекстной таблицы.
DeviceCustomString1	Название ключа записи.
DeviceCustomString1Label	key
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Контекстная таблица успешно очищена или операция завершилась с ошибкой

События аудита по контекстным таблицам создаются только для действий, совершенных пользователями.

Событию может быть присвоен статус succeeded или failed.

Поскольку запрос на очистку контекстной таблицы осуществляется через удаленное соединение, ошибка передачи данных может возникнуть в любой момент: до удаления или после удаления.

Это означает, что контекстная таблица может быть очищена успешно, но событие все равно будет иметь статус failed, поскольку EventOutcome возвращает статус TCP/IP-соединения запроса, а не статус проверки, была ли очищена контекстная таблица.

Значения полей события аудита Контекстная таблица успешно очищена или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	context table cleared
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для очистки контекстной таблицы.
SourceUserID	Идентификатор пользователя, который использовался для очистки контекстной таблицы.
DeviceExternalID	Идентификатор сервиса, контекстная таблица которого была очищена.
ExternalID	Идентификатор контекстной таблицы.
Name	Название контекстной таблицы.
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Ресурс добавлен

Название поля события	Значение поля
DeviceAction	resource added
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для добавления ресурса.
SourceUserID	Идентификатор пользователя, который использовался для добавления ресурса.
DeviceExternalID	Идентификатор ресурса.
DeviceProcessName	Название ресурса.
DeviceFacility	Тип ресурса: • activeList • agent • aggregationRule • collector • connection • connector • correlationRule • correlator • destination • dictionary • enrichmentRule • filter • normalizer • proxy • responseRule • storage
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Ресурс удален

Название поля события	Значение поля
DeviceAction	resource deleted
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.

SourceUserName	Логин пользователя, который использовался для удаления ресурса.
SourceUserID	Идентификатор пользователя, который использовался для удаления ресурса.
DeviceExternalID	Идентификатор ресурса.
DeviceProcessName	Название ресурса.
DeviceFacility	Тип ресурса: • activeList • agent • aggregationRule • collector • connection • connector • correlationRule • correlator • destination • dictionary • enrichmentRule • filter • normalizer • proxy • responseRule • storage
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Ресурс обновлен

Название поля события	Значение поля
DeviceAction	resource updated
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для обновления ресурса.
SourceUserID	Идентификатор пользователя, который использовался для обновления ресурса.
DeviceExternalID	Идентификатор ресурса.
DeviceProcessName	Название ресурса.

DeviceFacility	Тип ресурса: • activeList • agent • aggregationRule • collector • connection • connector • correlationRule • correlator • destination • dictionary • enrichmentRule • filter • normalizer • proxy • responseRule • storage
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Импорт ресурсов

Название поля события	Значение поля
DeviceAction	import resources
EventOutcome	succeeded
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который импортировал ресурсы.
SourceUserID	Идентификатор пользователя, который импортировал ресурсы.
DeviceCustomString5	Идентификатор тенанта, в который импортировали ресурсы.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта, в который импортировали ресурсы.
DeviceCustomString6Label	tenant name
FileType	Источник импорта: file или repository.
FileID	Если ресурсы импортированы из репозитория, идентификатор пакета. Если ресурсы импортированы из файла, системный идентификатор файла.
ExternalID	Если ресурсы импортированы из репозитория, версия импортированного пакета. Если ресурсы импортированы из файла, пустое значение.

Параметры обновлены

Название поля события	Значение поля
DeviceAction	settings updated
EventOutcome	succeeded

SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который использовался для обновления параметров.
SourceUserID	Идентификатор пользователя, который использовался для обновления параметров.
DeviceFacility	Тип параметров.
DeviceCustomString1	JSON с пороговыми значениями, записанными в базу данных.
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Словарь успешно обновлен на сервисе или операция завершилась ошибкой

Название поля события	Значение поля
DeviceAction	`dictionary update succeeded`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для создания сервиса.
SourceUserID	Идентификатор пользователя, который использовался для создания сервиса.
DeviceExternalID	Идентификатор сервиса.
ExternalID	Идентификатор словаря.
DeviceProcessName	Имя сервиса.
DeviceFacility	Тип сервиса.
DeviceCustomString1	Тип словаря: таблица, словарь.
DeviceCustomString1Label	`dictionary type`
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.

Запись добавлена в словарь

Выполнено добавление или обновление записи в словаре через API.

Значения полей события аудита Запись добавлена в словарь

Название поля события	Значение поля
DeviceAction	dictionary item added
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который добавил запись.
SourceUserID	Идентификатор пользователя, который добавил запись.
DeviceExternalID	Идентификатор сервиса.
ExternalID	Идентификатор словаря.
DeviceProcessName	Имя сервиса.
DeviceFacility	Тип сервиса.
DeviceCustomString1	Тип словаря: таблица, словарь.
DeviceCustomString1Label	dictionary type
DeviceCustomString2	Ключ записи.
DeviceCustomString2Label	key
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Запись успешно удалена из словаря или операция завершилась с ошибкой

Выполнено удаление записи из словаря (для типов: таблица, словарь) через API.

Событию может быть присвоен статус `succeeded` или `failed`.

Значения полей события аудита Запись успешно удалена из словаря или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceAction	dictionary item deleted
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.

SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который удалял запись из словаря.
SourceUserID	Идентификатор пользователя, который удалял запись из словаря.
DeviceExternalID	Идентификатор сервиса, запись в словаре которого была удалена.
ExternalID	Идентификатор словаря.
DeviceProcessName	Имя сервиса.
DeviceFacility	Тип сервиса.
DeviceCustomString1	Тип словаря: таблица, словарь.
DeviceCustomString1Label	dictionary type
DeviceCustomString2	Ключ записи.
DeviceCustomString2Label	key
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString5	Идентификатор тенанта сервиса. Некоторые ошибки не позволяют добавить информацию о тенанте в событие.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Создание поля расширенной схемы события

Название поля события	Значение поля
DeviceAction	extended field created
EventOutcome	succeeded
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который создал поле расширенной схемы события.
SourceUserID	Идентификатор пользователя, который создал поле расширенной схемы события.
DeviceCustomString5	Полное имя поля (SA.sting_array).

Редактирование поля расширенной схемы события

Название поля события	Значение поля
DeviceAction	extended field edited
EventOutcome	succeeded
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.

SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который редактировал поле расширенной схемы события.
SourceUserID	Идентификатор пользователя, который редактировал поле расширенной схемы события.
DeviceCustomString5	Полное имя поля (SA.sting_array).

Импорт поля расширенной схемы события

Название поля события	Значение поля
DeviceAction	extended field imported
EventOutcome	succeeded
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который импортировал поле расширенной схемы события.
SourceUserID	Идентификатор пользователя, который импортировал поле расширенной схемы события.
DeviceCustomString5	Полное имя поля (SA.sting_array).

Импорт нормализатора с полем расширенной схемы события

Название поля события	Значение поля
DeviceAction	extended field imported
EventOutcome	succeeded
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который импортировал нормализатор с полем расширенной схемы события.
SourceUserID	Идентификатор пользователя, который импортировал нормализатор с полем расширенной схемы события.
DeviceCustomString5	Полное имя поля (SA.sting_array).

Удаление поля расширенной схемы события

Название поля события	Значение поля
DeviceAction	extended field deleted
EventOutcome	succeeded
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.

SourceUserName	Логин пользователя, который удалил поле расширенной схемы события.
SourceUserID	Идентификатор пользователя, который удалил поле расширенной схемы события.
DeviceCustomString5	Полное имя поля (SA.sting_array).

Отправлен запрос в KIRA

Название поля события	Значение поля
DeviceAction	KIRA task
EventOutcome	succeeded/ failed
SourceUserName	Логин пользователя, который использовался для отправки запроса.
SourceUserID	Идентификатор пользователя, который использовался для отправки запроса.
DeviceCustomString1	Итоговая отправленная строка.
DeviceCustomString1Label	cmd
DeviceCustomString2	Идентификатор события, из которого отправлен запрос.
DeviceCustomString2Label	event
DeviceCustomString3	Идентификатор задачи, созданной для отправки запроса.
DeviceCustomString3Label	task

Реагирование через KICS/KATA

Название поля события	Значение поля
DeviceAction	KICS response
DeviceAssetID	asset fqdn
DeviceFacility	manual response или automatic response
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который отправил запрос.
SourceUserID	Идентификатор пользователя, который отправил запрос.
DeviceCustomString3	Наименование правила ответа: Authorized, Not Authorized.
DeviceCustomString3Label	response rule name
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name
DeviceExternalID	Идентификатор актива.

SourceHostName	FQDN актива.
Name	Название актива.
DeviceCustomString1	Перечень ip-адресов актива.
DeviceCustomString1Label	addresses
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.
DeviceCustomString2	fdqn
DeviceCustomString2Label	fqdns

Реагирование через Kaspersky Automated Security Awareness Platform

Название поля события	Значение поля
DeviceAction	KASAP response
DeviceFacility	manual response
EventOutcome	succeeded или failed
Message	Описание ошибки, если произошла ошибка, иначе поле будет пустое.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который отправил запрос.
SourceUserID	Идентификатор пользователя, который отправил запрос.
DeviceCustomString1	Менеджер пользователя, на которого назначен курс.
DeviceCustomString1Label	manager
DeviceCustomString3	Информация о группе, где был пользователь. Отсутствует в случае failed.
DeviceCustomString3Label	manager
DeviceCustomString4	Информация о группе, куда добавили пользователя.
DeviceCustomString4Label	new kasap group
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name
DestinationUserID	Идентификатор учетной записи пользователя Active Directory, на которую происходит реагирование.
DestinationUserName	Имя учетной записи (sAMAccountName).
DestinationNtDomain	Домен учетной записи пользователя Active Directory, на которую происходит реагирование.

Реагирование через KEDR

Название поля события	Значение поля
DeviceAction	KEDR response
DeviceFacility	manual response или automatic response
EventOutcome	succeeded или failed
Message	Описание ошибки, если произошла ошибка, иначе поле будет пустое.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который отправил запрос.
SourceUserID	Идентификатор пользователя, который отправил запрос.
SourceAssetID	Идентификатор актива в Kaspersky SIEM Cloud, для которого производится реагирование. Значение не указывается, если реагирование производится по хешу или для всех активов.
DeviceExternalID	Параметр external ID, присвоенный Kaspersky SIEM Cloud в KEDR. Если external id один, при запуске по пользовательским хостам не заполняется.
DeviceCustomString1	Перечисление IP/FQDN-адресов актива для правила запрета для хоста по выбранному хешу из карточки события.
DeviceCustomString1Label	user defined list of ips or hostnames
DeviceCustomString2	Параметр sensor ID в KEDR (UUIDv4 | 'all' | 'custom').
DeviceCustomString2Label	sensor id of asset in KATA/EDR
ServiceID	Идентификатор сервиса, который вызвал реагирование. Заполняется только при автоматическом реагировании.
DeviceCustomString3	Наименование типа задачи: enable_network_isolation, disable_network_isolation, enable_prevention, disable_prevention, run_process.
DeviceCustomString3Label	kedr response kind
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Импорт техник и тактик MITRE ATT&CK

Название поля события	Значение поля
DeviceAction	import MITRE
EventOutcome	succeeded
FileID	Имя импортируемого файла.
SourceUserID	Идентификатор пользователя, который отправил запрос на импорт.
SourceUserName	Логин пользователя, который отправил запрос на импорт.

Зарегистрирован алерт Metrics для сервиса или операция завершилась с ошибкой

Название поля события	Значение поля
DeviceProcessName	Имя сервиса.
DeviceFacility	Тип сервиса.
DeviceExternalID	Идентификатор сервиса.
DeviceCustomString6Label	tenant name
DeviceCustomString6	Название тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString2Label	Возможные значения: • QPS threshold reached • Failed Insert QPS threshold reached • High distribution queue • Low disk space • Low disk partition space • Output EventLoss increasing • Disk buffer size increasing • Enrichment errors increasing • High enrichment queue • Connector log errors increasing
DeviceCustomString2	created (время создания сервиса)
DeviceCustomString1Label	Порт API.
DeviceCustomNumber1	Продолжительность работы в секундах.
DeviceAction	service alert
EventOutcome	succeeded или failed

Реагирование в Active Directory

Название поля события	Значение поля
DeviceAction	ad response
DeviceFacility	manual response или automatic response
EventOutcome	succeeded или failed
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который применил реагирование.
SourceUserID	Идентификатор пользователя, который применил реагирование.
DeviceCustomString3	Наименование правила реагирования: CHANGE_PASSWORD, ADD_TO_GROUP, REMOVE_FROM_GROUP, BLOCK_USER.

DeviceCustomString3Label	response rule name
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name
DestinationUserName	Учетная запись пользователя Active Directory, на которую вызван ответ (sAMAccountName).
DestinationNtDomain	Домен учетной записи пользователя Active Directory, на которую вызван ответ.
DestinatinUserID	UUID учетной записи в KUMA.
FlexString1	Информация о группе, куда был добавлен или удален пользователь.
FlexString1Label	group DN

Резервное копирование партиций, восстановление из резервной копии, импорт партиций из сторонней установки Kaspersky SIEM Cloud

Название поля события	Значение поля
DeviceAction	backup/restore/import
EventOutcome	succeeded или failed
SourceUserName	Логин пользователя, который выполнял резервное копирование партиций, восстановление из резервной копии или импорт партиций из сторонней установки Kaspersky SIEM Cloud.
SourceUserID	Идентификатор пользователя, который выполнял резервное копирование партиций, восстановление из резервной копии или импорт партиций из сторонней установки Kaspersky SIEM Cloud.
DeviceExternalID	Идентификатор сервиса хранилища.
Name	Имя хранилища.
FilePath	Полный путь хранения файла резервной копии. Полный путь, откуда должен быть выполнено восстановление из резервной копии или импорт партиций.
Message	Если EventOutcome = failed, в этом поле будет отображаться сообщение об ошибке.

Запрос на естественном языке отправленный для преобразования в SQL-запрос с использованием KIRA

Название поля события	Значение поля
DeviceAction	KIRA request
EventOutcome	succeeded/ failed
SourceUserName	Логин пользователя, который использовался для отправки запроса.
SourceUserID	Идентификатор пользователя, который использовался для отправки запроса.
DeviceCustomString1	Итоговая отправленная строка.
DeviceCustomString1Label	sql text

Попытка чтения событий

Название поля события	Значение поля
DeviceAction	event search
Name	Чтение журналов.
EventOutcome	succeeded или failed
SourceUserName	Логин пользователя, который выполнил поисковый запрос.
SourceUserID	Идентификатор пользователя, который выполнил поисковый запрос.
DeviceCustomString3	Список выбранных пользователем пространств хранилища в разделе **События**.
DeviceCustomString3Label	space name
DeviceCustomString4	Текст поискового запроса.
DeviceCustomString4Label	text of the search query

Поисковый запрос отменен

Поле Message может отсутствовать.

Название поля события	Значение поля
DeviceAction	canceling a search query
Message	Причина отмены запроса.
Name	Поисковый запрос отменен.
DeviceCustomString5	Идентификатор тенанта сервиса (при некоторых ошибках информация о тенанте может отсутствовать).
DeviceCustomString3Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name
DeviceExternalID	Идентификатор хранилища.
EventOutcome	succeeded или failed
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который выполнил поисковый запрос.
SourceUserID	Идентификатор пользователя, который выполнил поисковый запрос.

Ресурсы KEDR обновлены

Название поля события	Значение поля
DeviceAction	resource updated
EventOutcome	succeeded или failed

DeviceExternalID	Идентификатор ресурса.
DeviceProcessName	Имя ресурса.
DeviceFacility	Тип ресурса.
DeviceCustomNumber2	Версия ресурса (число).
DeviceCustomNumber2Label	EDR resource version
DeviceCustomString4	Версия Kaspersky SIEM Cloud.
DeviceCustomString4Label	Kaspersky SIEM Cloud version
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenantID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Задача обновления ресурсов KEDR завершена

Название поля события	Значение поля
DeviceAction	Apply EDR resources task
Message	Устаревшие ресурсы EDR обновлены. Сервисы с обновленными ресурсами EDR перезагружены.
EventOutcome	succeeded или failed
DeviceCustomNumber1	Название ресурса коллектора.
DeviceCustomNumber1Label	reloaded collectors
DeviceCustomNumber3	Название ресурса коррелятора.
DeviceCustomNumber3Label	reloaded correlators
DeviceCustomString4	Версия Kaspersky SIEM Cloud.
DeviceCustomString4Label	Kaspersky SIEM Cloud version
DeviceCustomString5	Имя ресурса.
DeviceCustomString5Label	imported resources

Поля события KEDR обновлены

Название поля события	Значение поля
DeviceAction	Apply EDR resources task
Message	Новые расширенные поля EDR применены.
EventOutcome	succeeded или failed
DeviceCustomNumber1	Версия расширенных полей событий.
DeviceCustomNumber1Label	New EDR fields version
DeviceCustomString4	Версия Kaspersky SIEM Cloud.
DeviceCustomString4Label	Kaspersky SIEM Cloud version

Файл localizations.json обновлен

Название поля события	Значение поля
DeviceAction	Import IOA rules localizations
EventOutcome	succeeded или failed
DeviceCustomDate1	dd.mm.yyy hh:mm:ss
DeviceCustomDate1Label	Last update IoA rules localizations file content

Правило привязано к коллектору

Название поля события	Значение поля
DeviceAction	link rule to collector
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который изменил данные.
SourceUserID	Идентификатор пользователя, который изменил данные.
ExternalID	Идентификатор сервиса, к которому было привязано правило.
Name	Имя сервиса, к которому было привязано правило.
DeviceFacility	Действие (правило привязано).
DeviceCustomString1	Идентификатор правила.
DeviceCustomString1Label	rule ID
DeviceCustomString2	Имя правила.
DeviceCustomString2Label	rule name
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Правило отвязано от коллектора

Название поля события	Значение поля
DeviceAction	unlink rule from collector
EventOutcome	succeeded

SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который изменил данные.
SourceUserID	Идентификатор пользователя, который изменил данные.
ExternalID	Идентификатор сервиса, от которого было отвязано правило.
Name	Имя сервиса, от которого было отвязано правило.
DeviceFacility	Действие (правило отвязано).
DeviceCustomString1	Идентификатор правила.
DeviceCustomString1Label	`rule ID`
DeviceCustomString2	Имя правила.
DeviceCustomString2Label	`rule name`
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	`tenant name`

Правило привязано к коррелятору

Название поля события	Значение поля
DeviceAction	`link rule to correlator`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка `x-real-ip` или `x-forwarded-for`. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который изменил данные.
SourceUserID	Идентификатор пользователя, который изменил данные.
ExternalID	Идентификатор сервиса, к которому было привязано правило.
Name	Имя сервиса, к которому было привязано правило.
DeviceFacility	Действие (правило привязано).
DeviceCustomString1	Идентификатор правила.
DeviceCustomString1Label	`rule ID`
DeviceCustomString2	Имя правила.
DeviceCustomString2Label	`rule name`
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	`tenant ID`

DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Правило отвязано от коррелятора

Название поля события	Значение поля
DeviceAction	unlink rule from correlator
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который изменил данные.
SourceUserID	Идентификатор пользователя, который изменил данные.
ExternalID	Идентификатор сервиса, от которого было отвязано правило.
Name	Имя сервиса, от которого было отвязано правило.
DeviceFacility	Действие (правило отвязано).
DeviceCustomString1	Идентификатор правила.
DeviceCustomString1Label	rule ID
DeviceCustomString2	Имя правила.
DeviceCustomString2Label	rule name
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Экспорт ресурсов из Kaspersky SIEM Cloud

Для каждого экспортируемого ресурса создается отдельное событие аудита.

Название поля события	Значение поля
DeviceAction	export resources
EventOutcome	succeeded
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси-сервер, будет указан порт прокси-сервера.
SourceUserName	Логин пользователя, который экспортировал ресурсы.

SourceUserID	Идентификатор пользователя, который экспортировал ресурсы.
DeviceCustomString5	Идентификатор тенанта, из которого были экспортированы ресурсы.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Идентификатор ресурса, который был экспортирован.
DeviceCustomString6Label	resource ID
DeviceCustomString4	Версия ресурса, который был экспортирован.
DeviceCustomString4Label	version

Получение служебных данных о событиях из изолированного сегмента

Служебные данные о событиях передаются в коллектор по протоколу internal. Для передачи таких данных из изолированного сетевого сегмента используется выделенный агент, установленный внутри этого сегмента.

Для передачи данных от агента в коллектор по протоколу internal между агентом и коллектором должна произойти взаимная аутентификация с помощью сертификатов. Вы можете создать и сохранить сертификат агента в конфигурационный файл агента и затем использовать этот файл для установки агента в изолированном сегменте. Данные о сертификате сохраняются в файле в зашифрованном виде.

Чтобы настроить получение служебных данных о событиях из изолированного сегмента:

1. Создайте или настройте коллектор с коннектором internal.
2. Создайте агент и настройте передачу данных в коллектор:
   a. В веб-консоли в разделе **Мониторинг** → **Ресурсы и сервисы** → **Агенты** нажмите **Создать**.
   b. В открывшемся окне **Создание агента** на вкладке **Общие параметры** задайте параметры **Название** и **Тенант**.
   c. На вкладке **Подключение №{{index}}** в блоке **Коннектор** укажите следующие параметры:
      - **Название** – укажите название коннектора.
      - **Тип** – укажите тип коннектора.
      - **URL** – укажите хост, на котором будет установлен агент для получения событий.
   d. На вкладке **Подключение №{{index}}** в блоке **Точки назначения** укажите следующие параметры:
      - **Название** – укажите название точки назначения.
      - **Тип** – укажите протокол **internal**, по которому будет выполняться передача событий.
      - **URL** – укажите хост, на котором установлен коллектор с коннектором **internal**.
   e. Нажмите **Создать**.

f. Выберите из списка созданный набор ресурсов агента и затем в окне свойств агента нажмите **Скачать конфигурацию, содержащую сертификат**. В открывшемся окне задайте пароль, который будет использован для шифрования сертификата, а также будет запрашиваться при запуске агента.

   Конфигурация параметров агента скачивается в виде JSON-файла в соответствии с параметрами вашего браузера. Этот файл используется при установке агента в изолированном сегменте сети.

   > Необходимо при помощи списка контроля доступа (ACL) настроить права доступа к файлу на сервере, где будет установлен агент. Чтение файла должно быть доступно пользователю, от имени которого будет запускаться агент.

g. Установите агент в изолированном сегменте сети. Установка возможна на устройствах Linux и Windows.

Настройка получения служебных данных о событиях из изолированного сегмента завершена.

Ребалансировка хранилища запущена

Название поля события	Значение поля
DeviceAction	storage rebalance started
EventOutcome	succeeded
Name	Кластер хранилища.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
DeviceExternalID	Идентификатор сервиса.
SourceUserID	Идентификатор пользователя, который выполнил команду.
SourceUserName	admin
DeviceCustomString1	3,4
DeviceCustomString1Label	target shards
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Ребалансировка успешно завершена

Название поля события	Значение поля
DeviceAction	storage rebalance completed
EventOutcome	succeeded
Name	Кластер хранилища.
DeviceExternalID	Идентификатор сервиса.
SourceServiceName	scheduler

DeviceCustomString1	3,4
DeviceCustomString1Label	target shards

Запрос остановки ребалансировки хранилища

Название поля события	Значение поля
DeviceAction	storage rebalance stop requested
EventOutcome	succeeded
Name	Кластер хранилища.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси-сервера, будет указан адрес прокси-сервера.
DeviceExternalID	Идентификатор сервиса.
SourceUserID	Идентификатор пользователя, который выполнил команду.
SourceUserName	admin
DeviceCustomString1	Целевые шарды.
DeviceCustomString1Label	
DeviceCustomString5	Идентификатор тенанта.
DeviceCustomString5Label	tenant ID
DeviceCustomString6	Название тенанта.
DeviceCustomString6Label	tenant name

Ребалансировка завершилась ошибкой

Название поля события	Значение поля
DeviceAction	storage rebalance failed
EventOutcome	failed
Name	Кластер хранилища.
DeviceExternalID	Идентификатор сервиса.
SourceServiceName	scheduler
DeviceCustomString1	3,4
DeviceCustomString1Label	target shards
Message	Unexpected partition move state: partition ID is empty или Unexpected partition move state: detached partition is absent

Правила корреляции

В файле, доступном по ссылке для скачивания, описаны правила корреляции, включенные в поставку. Приводятся сценарии, покрываемые правилами, условия их использования и необходимые источники событий.

Описанные в этом документе правила корреляции содержатся в файле SOC_package дистрибутива OSMP и защищены паролем SOC_package1. Одновременно возможно использование только одной версии набора SOC-правил: или русской, или английской.

Импортированные правила корреляции можно добавлять в используемые вашей организацией корреляторы. Дополнительную информацию см. в разделе: Шаг 3. Корреляция.

Чтобы импортировать пакет правил корреляции в KUMA:

1. В разделе KUMA Консоли OSMP перейдите в раздел **Параметры** → **Обновление хранилища** и для параметра **Источник обновлений** установите значение **Серверы обновлений "Лаборатории Касперского"**.

   Вы также можете настроить обновление хранилища.

2. Нажмите на **Запустить обновление**, чтобы сохранить параметры обновления и вручную запустить задачу *Обновление хранилища*.

3. Перейдите в **Диспетчер задач,** чтобы убедиться, что задача *Обновление хранилища* завершена.

4. Перейдите в раздел **Ресурсы** и нажмите на **Импортировать ресурсы**.

5. В окне **Импортировать ресурсы** выберите тенант, которому будут принадлежать импортируемые ресурсы.

6. В раскрывающемся списке **Импортировать ресурсы** выберите **Хранилище**, выберите пакет SOC Content и нажмите на **Импортировать**.

   Ресурсы из пакета SOC Content импортируются в KUMA. Дополнительные сведения об импорте см. в разделе Импорт ресурсов.

Скачать описание правил корреляции, содержащихся в файле SOC_package.xlsx.

Фильтры

Фильтры позволяют отбирать события на основании указанных условий. Вы можете использовать фильтры в коллекторах, корреляторах, хранилище, правилах корреляции, правилах обогащения, правилах агрегации, точках назначения, правилах реагирования и правилах сегментации. В сервисе коллектора фильтры используются для отображения событий, которые вы хотите передавать в Kaspersky SIEM Cloud. События, удовлетворяющие условиям фильтра, будут переданы в Kaspersky SIEM Cloud для дальнейшей обработки.

Вы можете использовать отдельные фильтры или встроенные фильтры, которые хранятся в сервисе или ресурсе, в котором они были созданы. Для ресурсов в полях ввода, кроме поля **Описание**, можно включить отображение непечатаемых символов.

Для ресурсов, использованных в фильтре, автоматически указывается их наименование. Поля, содержащие наименования связанных ресурсов, невозможно изменить. Названия категорий общих ресурсов не отображаются в фильтре, если вам не назначена роль Чтение общих ресурсов. Для просмотра списка ресурсов для выбранного операнда внутри выражения вам нужно нажать на комбинацию клавиш **Ctrl+Space**. В результате отобразится список ресурсов.

Чтобы просмотреть фильтры,

в веб-консоли откройте раздел **Мониторинг → Ресурсы и сервисы → Фильтры**.

Откроется таблица фильтров.

Фильтры можно искать по названию с помощью поля **Поиск**. При поиске фильтров используются регулярные выражения.

Таблицу можно сортировать по названию, времени последнего обновления и по названию пакета, нажав на значок сортировки ⌄ в заголовке столбца и выбрав **По возрастанию** или **По убыванию**.

Таблица фильтров содержит следующие столбцы:

- **Название** – название фильтра.
- **Путь до ресурса** – тенант, которому принадлежит фильтр.
- **Последнее обновление** – дата и время последнего обновления фильтра.
- **Создал** – имя пользователя, создавшего фильтр.
- **Описание** – информация о фильтре, которую вы можете добавить при необходимости.
- **Теги** – теги для поиска фильтра. Вы можете искать фильтры, нажав на значок сортировки в заголовке столбца и указав значение для поиска в поле **Поиск** или выбрав теги с помощью флажков.
- **Название пакета** – название пакета инструментов, предназначенного для обработки событий.

При создании фильтра необходимо указать операнды и операторы. Доступные типы операторов зависят от выбранного левого (L) и/или правого (R) операндов.

Доступные типы операторов для левого (L) и правого (R) операндов

Оператор	Тип "Поля событий"	Тип "Активные листы"	Тип "Словари"	Тип "Контекстные таблицы"	Тип "Таблицы"	Тип "TI"	Тип "Константа"	Тип "Список"
=	L, R	L, R	L, R	L, R	L, R	L, R	R	R
>	L, R	L, R	L, R	L, R (только при поиске значения таблицы по индексу)	L, R	L	R	—
>=	L, R	L, R	L, R	L, R (только при поиске значения таблицы по индексу)	L, R	L	R	—

<	L, R	L, R	L, R	L, R (только при поиске значения таблицы по индексу)	L, R	L	R	—
<=	L, R	L, R	L, R	L, R (только при поиске значения таблицы по индексу)	L, R	L	R	—
inSubnet	L, R	L, R	L, R	L, R	L, R	L, R	R	R
contains	L, R	L, R	L, R	L, R	L, R	L, R	R	R
startsWith	L, R	L, R	L, R	L, R	L, R	L, R	R	R
endsWith	L, R	L, R	L, R	L, R	L, R	L, R	R	R
match	L	L	L	L	L	L	R	R
hasVulnerability	L	L	L	L	L	—	—	—
hasBit	L	L	L	L	L	—	R	R
inActiveList	—	—	—	—	—	—	—	—
inDictionary	—	—	—	—	—	—	—	—
inCategory	L	L	L	L	L	—	R	R
inContextTable	—	—	—	—	—	—	—	—
inActiveDirectoryGroup	L	L	L	L	L	—	R	R
TIDetect	—	—	—	—	—	—	—	—

Горячие клавиши при работе с фильтрами

При работе с фильтрами вы можете использовать горячие клавиши (см. таблицу ниже).

Горячие клавиши и их функциональность

Клавиша	Функциональность
e	Вызывает фильтр по полю события.
d	Вызывает фильтр по полю словаря.
a	Вызывает фильтр по полю активного листа.
c	Вызывает фильтр по полю контекстной таблицы.
t	Вызывает фильтр по полю таблицы.
f	Вызывает фильтр.
t+i	Вызывает фильтр с использованием TI.
Ctrl+Enter	Завершение редактирования условия.

Фильтры с расширенной схемой событий

Работа с полями типа `Строка`, `Число` и **Число с плавающей точкой** расширенной схемы событий в фильтрах не отличается от работы с полями схемы событий Kaspersky SIEM Cloud.

При использовании фильтров с полями расширенной схемы событий с типами полей `Массив строк`, `Массив целых чисел` и `Массив чисел с плавающей точкой` вы можете использовать следующие операторы:

- **contains** вернет значение `True`, если указанная подстрока присутствует в массиве, иначе вернет `False`.
- **match** – поиск в строке по регулярному выражению.
- **intersec**.

Предустановленные фильтры

В поставку Kaspersky SIEM Cloud включены перечисленные в таблице ниже фильтры.

Предустановленные фильтры

Название фильтра	Описание
[OOTB][AD] A member was added to a security-enabled global group (4728)	Выбирает события добавления пользователя в группу безопасности (security-enabled global group) Active Directory.
[OOTB][AD] A member was added to a security-enabled universal group (4756)	Выбирает события добавления пользователя в группу безопасности (security-enabled universal group) Active Directory.
[OOTB][AD] A member was removed from a security-enabled global group (4729)	Выбирает события удаления пользователя из группы безопасности (security-enabled global group) Active Directory.
[OOTB][AD] A member was removed from a security-enabled universal group (4757)	Выбирает события удаления пользователя из группы безопасности (security-enabled universal group) Active Directory.
[OOTB][AD] Account Created	Выбирает события создания учетной записи в операционной системе Windows.
[OOTB][AD] Account Deleted	Выбирает события удаления учетной записи в операционной системе Windows.
[OOTB][AD] An account failed to log on (4625)	Выбирает события безуспешной попытки входа в операционной системе Windows.
[OOTB][AD] Successful Kerberos authentication (4624, 4768, 4769, 4770)	Выбирает события успешной попытки входа в операционной системе Windows и события с идентификаторами 4769, 4770, регистрирующиеся на контроллерах домена.
[OOTB][AD][Technical] 4768. TGT Requested	Выбирает события Microsoft Windows с идентификатором 4768.
[OOTB][Net] Possible port scan	Выбирает события, которые могут говорить о проведении сканирования портов.
[OOTB][SSH] Accepted Password	Выбирает события успешного подключения с использованием пароля по протоколу SSH.
[OOTB][SSH] Failed Password	Выбирает события попыток подключения с использованием пароля по протоколу SSH.

Формат времени

Kaspersky SIEM Cloud поддерживает обработку информации, передающейся в поля Модели данных события с типом timestamp (EndTime, StartTime, DeviceCustomDate1, и т.д.) в следующих форматах:

- "May 8, 2009 5:57:51 PM",
- "oct 7, 1970",
- "oct 7, '70",
- "oct. 7, 1970",
- "oct. 7, 70",

- "Mon Jan 2 15:04:05 2006",
- "Mon Jan 2 15:04:05 MST 2006",
- "Mon Jan 02 15:04:05 -0700 2006",
- "Monday, 02-Jan-06 15:04:05 MST",
- "Mon, 02 Jan 2006 15:04:05 MST",
- "Tue, 11 Jul 2017 16:28:13 +0200 (CEST)",
- "Mon, 02 Jan 2006 15:04:05 -0700",
- "Mon 30 Sep 2018 09:09:09 PM UTC",
- "Mon Aug 10 15:44:11 UTC+0100 2015",
- "Thu, 4 Jan 2018 17:53:36 +0000",
- "Fri Jul 03 2015 18:04:07 GMT+0100 (GMT Daylight Time)",
- "Sun, 3 Jan 2021 00:12:23 +0800 (GMT+08:00)",
- "September 17, 2012 10:09 am",
- "September 17, 2012 at 10:09 am PST-08",
- "September 17, 2012, 10:10:09",
- "October 7, 1970",
- "October 7th, 1970",
- "12 Feb 2006, 19:17",
- "12 Feb 2006 19:17",
- "14 May 2019 19:11:40.164",
- "7 oct 70",
- "7 oct 1970",
- "03 February 2013",
- "1 July 2013",
- "2013-Feb-03".

Формат dd/Mon/yyyy

- "06/Jan/2008:15:04:05 -0700",
- "06/Jan/2008 15:04:05 -0700".

Формат mm/dd/yyyy

- "3/31/2014",
- "03/31/2014",
- "08/21/71",
- "8/1/71",
- "4/8/2014 22:05",
- "04/08/2014 22:05",
- "4/8/14 22:05",
- "04/2/2014 03:00:51",
- "8/8/1965 12:00:00 AM",
- "8/8/1965 01:00:01 PM",
- "8/8/1965 01:00 PM",
- "8/8/1965 1:00 PM",
- "8/8/1965 12:00 AM",
- "4/02/2014 03:00:51",
- "03/19/2012 10:11:59",
- "03/19/2012 10:11:59.3186369".

Формат yyyy/mm/dd

- "2014/3/31",
- "2014/03/31",
- "2014/4/8 22:05",

- "2014/04/08 22:05",
- "2014/04/2 03:00:51",
- "2014/4/02 03:00:51",
- "2012/03/19 10:11:59",
- "2012/03/19 10:11:59.3186369".

Формат yyyy:mm:dd

- "2014:3:31",
- "2014:03:31",
- "2014:4:8 22:05",
- "2014:04:08 22:05",
- "2014:04:2 03:00:51",
- "2014:4:02 03:00:51",
- "2012:03:19 10:11:59",
- "2012:03:19 10:11:59.3186369".

Формат, содержащий китайские символы

"2014年04月08日"

Формат yyyy-mm-ddThh

- "2006-01-02T15:04:05+0000",
- "2009-08-12T22:15:09-07:00",
- "2009-08-12T22:15:09",
- "2009-08-12T22:15:09.988",
- "2009-08-12T22:15:09Z",

- "2017-07-19T03:21:51:897+0100",
- "2019-05-29T08:41-04" без указания секунд, 2 символа TZ.

Формат yyyy-mm-dd hh:mm:ss

- "2014-04-26 17:24:37.3186369",
- "2012-08-03 18:31:59.257000000",
- "2014-04-26 17:24:37.123",
- "2013-04-01 22:43",
- "2013-04-01 22:43:22",
- "2014-12-16 06:20:00 UTC",
- "2014-12-16 06:20:00 GMT",
- "2014-04-26 05:24:37 PM",
- "2014-04-26 13:13:43 +0800",
- "2014-04-26 13:13:43 +0800 +08",
- "2014-04-26 13:13:44 +09:00",
- "2012-08-03 18:31:59.257000000 +0000 UTC",
- "2015-09-30 18:48:56.35272715 +0000 UTC",
- "2015-02-18 00:12:00 +0000 GMT",
- "2015-02-18 00:12:00 +0000 UTC",
- "2015-02-08 03:02:00 +0300 MSK m=+0.000000001",
- "2015-02-08 03:02:00.001 +0300 MSK m=+0.000000001",
- "2017-07-19 03:21:51+00:00",
- "2014-04-26",
- "2014-04",
- "2014",
- "2014-05-11 08:20:13,787".

Формат yyyy-mm-dd-07:00

"2020-07-20+08:00"

Формат mm.dd.yyyy

- "3.31.2014",
- "03.31.2014",
- "08.21.71".

Формат yyyy.mm.dd

"2014.03.30"

Формат yyyymmdd и аналогичные

- "20140601",
- "20140722105203".

Формат yymmdd hh:mm:yy

"171113 14:14:20"

Формат Unix timestamp

- "1332151919",
- "1384216367189",
- "13842163671111222",
- "138421636711122233 3".

Сопоставление полей предустановленных нормализаторов

В файле, доступном по ссылке для скачивания, представлено описание сопоставления полей предустановленных нормализаторов.

Скачать Описание сопоставления полей предустановленных нормализаторов

Юридическая информация

Лицензирование решения Kaspersky SIEM Cloud

Лицензия – это ограниченное по времени право на использование Kaspersky SIEM Cloud, предоставляемое вам на условиях заключенного Лицензионного соглашения. Объем предоставляемых услуг и срок использования решения зависят от типа лицензии, по которой используется решение.

Лицензия предоставляется при приобретении решения. Если лицензия отсутствует:

- По истечении срока действия лицензии Kaspersky SIEM Cloud в течение 7 суток работает без ограничений функциональности, то есть коллекторы продолжают принимать и обрабатывать события. По истечении 7 суток коллекторы и корреляторы перезагружаются и перестают принимать и обрабатывать новые события. Остальные запущенные сервисы продолжают работать. Сохраненные до прекращения приема события не удаляются и остаются доступны для поиска и просмотра в течение установленного срока хранения.
- Если лицензионный ключ удален, коллекторы Kaspersky SIEM Cloud сразу перестают принимать и обрабатывать новые события. Старые события остаются доступны.
- Невозможно создавать и редактировать ресурсы, создавать и запускать сервисы.

Активация решения

Для того чтобы активировать и затем использовать Kaspersky SIEM Cloud в соответствии с условиями Лицензионного соглашения, в решение необходимо добавить *лицензионный ключ*, который представляет собой уникальную последовательность бит. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Когда вы приобретаете решение, вам будет предоставлено два лицензионных ключа. Один лицензионный ключ позволяет активировать Kaspersky SIEM Cloud. Второй активирует в Kaspersky Endpoint Security возможность отправлять события операционной системы в коллекторы Kaspersky SIEM Cloud.

Вы можете добавить лицензионный ключ, применив *код активации*, который предоставляется вам после приобретения лицензии.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ, активирующий Kaspersky SIEM Cloud. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky SIEM Cloud.

Чтобы активировать решение с помощью кода активации, серверу с установленным Ядром Kaspersky SIEM Cloud требуется доступ в интернет для подключения к серверу активации "Лаборатории Касперского" по следующему адресу:

```
https://activation-v2.kaspersky.com:443
```

В случае закрытой инфраструктуры вы можете указать прокси-сервер.

Если код активации был потерян после активации Kaspersky SIEM Cloud, свяжитесь с партнером "Лаборатории Касперского", у которого вы приобрели лицензию.

При добавлении и удалении лицензионного ключа, а также при истечении срока действия лицензии, Kaspersky SIEM Cloud создает событие аудита.

Добавить лицензионный ключ вы можете в веб-интерфейсе решения в разделе **Лицензия**.

Лицензионный ключ отображается в веб-интерфейсе в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в решение.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы решения требуется добавить другой лицензионный ключ.

Лицензионный ключ, используемый в текущий момент для работы решения, становится *активным лицензионным ключом*. В решении не может быть больше одного активного лицензионного ключа.

Продление срока действия лицензии

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от угроз компьютерной безопасности.

Для своевременного продления срока действия лицензии вы можете предварительно добавить резервный лицензионный ключ.

Резервный лицензионный ключ – лицензионный ключ, подтверждающий право на использование Kaspersky SIEM Cloud, но не используемый в текущий момент. Резервный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом. Резервный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа. В качестве резервного лицензионного ключа не может быть использован лицензионный ключ для пробной лицензии.

О Лицензионном сертификате

Вместе с кодом активации вы также получаете *Лицензионный сертификат*, который содержит следующую информацию о предоставляемой лицензии:

- идентификатор лицензии или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о решении, которое можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, количество обрабатываемых событий в секунду);
- дата начала срока действия лицензии;

- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

Управление лицензионными ключами

В этой статье описано, как просмотреть информацию о лицензионных ключах, каким образом рассчитывается EPS, как добавить и удалить лицензионный ключ, заменить активный лицензионный ключ, добавить резервный лицензионный ключ.

О льготном периоде

Льготный период длится 7 дней и наступает в одном из следующих случаев:

- Вы удалили активный лицензионный ключ, при этом резервный лицензионный ключ не добавлен.

  В этом случае доступ к накопленным данным (например, событиям и алертам) блокируется.

- Срок действия активного лицензионного ключа истек, при этом резервный лицензионный ключ не добавлен.

  В этом случае доступ к накопленным данным (например, событиям и алертам) в течение льготного периода сохраняется.

Во время льготного периода применяются следующие ограничения:

- Не поступают новые события.
- Не создаются алерты и инциденты.
- Блокируется запуск плейбуков и все действия по реагированию, кроме следующих:
  - Отключение сетевой изоляции.
  - Восстановление файла из карантина.
  - Удаление правила запрета.

По истечении льготного периода все данные рабочей области удаляются без возможности восстановления. Данные не удаляются при выполнении одного из следующих условий:

- До истечения льготного периода добавлен действующий активный лицензионный ключ текущего решения.
- До истечения льготного периода добавлен действующий активный лицензионный ключ другого решения и пройдена активация решения.

Просмотр информации о лицензионных ключах

Лицензионные ключи применяются на уровне тенантов.

Чтобы просмотреть информацию о добавленных лицензионных ключах:

1. В главном окне приложения перейдите в раздел **Параметры** → **Тенанты** и нажмите на имя требуемого тенанта.

   Откроется окно свойств выбранного тенанта.

2. Перейдите на вкладку **Лицензии**.

В разделе отображается следующая информация:

- **Наименование лицензионного ключа** – название решения и уточняющие параметры, если применимо.
- Уникальная буквенно-цифровая последовательность лицензионного ключа.
- **Устройства** – текущее количество добавленных устройств и максимально возможное по лицензии количество устройств.
- **Учетные записи** – текущее количество добавленных учетных записей и максимально возможное по лицензии количество учетных записей.
- **Доступный EPS** – количество обрабатываемых в секунду событий, которое поддерживается лицензией.
- **Текущий EPS в день** – текущее среднее количество событий в секунду, рассчитанное по событиям, обработанным за доступный период наблюдения продолжительностью не более 24 часов.
- **Дата активации** – дата активации решения.
- **Срок действия** – дата истечения срока действия лицензионного ключа.
- **Условие** – количество дней до истечения срока действия лицензии.

Вы можете нажать на кнопку **Перейти к Серверу администрирования**, чтобы управлять лицензионными ключами.

Также можно просмотреть список модулей, доступных по лицензии. Для этого нажмите на кнопку ⓘ.

Расчет EPS

При расчете потока EPS учитываются только события, прошедшие нормализацию. События учитываются на выходе из коллектора после выполнения операций обработки, включая фильтрацию, агрегацию и обогащение. Если одно событие после обработки коллектором отправляется в несколько точек назначения, оно учитывается как одно событие.

Показатель **Текущий EPS в день** рассчитывается для всех лицензий. Показатель рассчитывается на основании количества событий, обработанных коллекторами за доступный период наблюдения продолжительностью не более 24 часов. Расчет выполняется по формуле:

```
(x1 + x2 + ... + xn) / (m Ч 3600) = EPS
```

где:

`x1, x2, ... xn` – количество событий, обработанных каждым коллектором за доступный период наблюдения.

`n` – количество коллекторов.

`m` – количество доступных часовых окон.

`3600` – количество секунд в одном часе.

Количество доступных часовых окон может быть меньше 24, например, если коллекторы начали работу менее 24 часов назад. В этом случае расчет выполняется по фактически доступным часовым окнам. Например, если коллекторы работают в течение трех часов, для расчета используются три часовых окна.

Превышение ограничения EPS

Если рассчитанное значение EPS превышает значение **Текущий EPS в день**, Kaspersky SIEM Cloud отображает информацию о превышении в разделе **Поиск угроз**.

Для лицензий с ограничением EPS на уровне тенанта при превышении этого ограничения Kaspersky SIEM Cloud также отображает информацию о превышении в разделе **Поиск угроз**. Значение 0 означает, что ограничение отсутствует.

Добавление активного лицензионного ключа

Чтобы добавить активный лицензионный ключ:

1. В главном окне приложения перейдите в раздел **Сервер администрирования → Общие → Лицензионные ключи**.
2. Нажмите на кнопку **Добавить**.

   Откроется список добавленных лицензионных ключей.
3. Выберите лицензионный ключ, который хотите использовать в качестве активного.

   Чтобы посмотреть детальную информацию о лицензионном ключе, нажмите на его буквенно-цифровую последовательность символов.

   Чтобы добавить в список новый лицензионный ключ, нажмите на кнопку **Добавить лицензионный ключ**, введите код активации и затем нажмите на кнопку **Отправить**.

4. Нажмите на кнопку **OK**.

5. В окне свойств Сервера администрирования нажмите **Сохранить**.

Активный лицензионный ключ добавлен.

Удаление лицензионного ключа

Вы можете удалить добавленный лицензионный ключ из Kaspersky SIEM Cloud (например, если вам нужно заменить активный лицензионный ключ другим). После удаления лицензионного ключа коллекторы сразу прекращают принимать и обрабатывать события. Старые события остаются доступны. Также невозможно создавать и изменять ресурсы, создавать и запускать сервисы. Эта работа возобновится после добавления лицензионного ключа.

Чтобы удалить лицензионный ключ:

1. В главном окне приложения перейдите в раздел **Сервер администрирования → Общие → Лицензионные ключи**.

2. Нажмите на кнопку **Удалить активный лицензионный ключ**.

   Откроется окно подтверждения.

3. Подтвердите удаление лицензионного ключа.

Лицензионный ключ будет удален

Замена активного лицензионного ключа

Если наименование нового лицензионного ключа не совпадает с наименованием текущего лицензионного ключа, набор доступных модулей и функций решения будет изменен в соответствии с новым лицензионным ключом.

Чтобы заменить активный лицензионный ключ:

1. В главном окне приложения перейдите в раздел **Сервер администрирования → Общие → Лицензионные ключи**.

2. Нажмите на кнопку **Изменить**.

   Откроется список добавленных лицензионных ключей.

3. Выберите лицензионный ключ, который хотите использовать в качестве активного.

   Чтобы посмотреть детальную информацию о лицензионном ключе, нажмите на его буквенно-цифровую последовательность символов.

   Чтобы добавить в список новый лицензионный ключ, нажмите на кнопку **Добавить лицензионный ключ**, введите код активации и затем нажмите на кнопку **Отправить**.

4. Нажмите на кнопку **OK**.

   Текущий лицензионный ключ будет заменен выбранным.

5. В окне свойств Сервера администрирования нажмите **Сохранить**.

Активный лицензионный ключ заменен.

Добавление резервного лицензионного ключа

Чтобы добавить резервный лицензионный ключ:

1. В главном окне приложения перейдите в раздел **Сервер администрирования → Общие → Лицензионные ключи**.

2. Нажмите на кнопку **Выбрать**.

   Откроется список добавленных лицензионных ключей.

3. Выберите лицензионный ключ, который хотите использовать в качестве резервного.

   Чтобы посмотреть детальную информацию о лицензионном ключе, нажмите на его буквенно-цифровую последовательность символов.

   Чтобы добавить в список новый лицензионный ключ, нажмите на кнопку **Добавить лицензионный ключ**, введите код активации и затем нажмите на кнопку **Отправить**.

4. Нажмите на кнопку **OK**.

5. В окне свойств Сервера администрирования нажмите **Сохранить**.

Резервный лицензионный ключ добавлен.

Лицензирование приложения Kaspersky Security Center Cloud Console

В этом разделе представлена информация, связанная с лицензированием приложения Kaspersky Security Center Cloud Console.

Лицензирование приложения Kaspersky Security Center Cloud Console

Следуя этому сценарию, вы можете приступить к использованию Kaspersky Security Center Cloud Console и управляемых приложений безопасности по лицензии.

Kaspersky Security Center Cloud Console позволяет централизованно распространять лицензионные ключи приложений "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.

Если вы уже используете Kaspersky Security Center Cloud Console, вы можете перейти в раздел Kaspersky Marketplace, который позволяет просмотреть весь спектр бизнес-решений "Лаборатории Касперского", выбрать те, которые нужны вам, и перейти к покупке на сайте "Лаборатории Касперского".

Ознакомление с функциями Kaspersky Security Center Cloud Console в пробном режиме перед покупкой лицензии

Вы можете сначала попробовать пробную версию Kaspersky Security Center Cloud Console. Для этого создайте пробную рабочую область, срок действия которой истекает через 30 дней. Если вам нужна коммерческая рабочая область, которую можно использовать столько, сколько нужно, вам нужно приобрести лицензию.

Этапы

Сценарий состоит из следующих этапов:

1. **Получение кода активации для лицензирования Kaspersky Security Center Cloud Console в коммерческом режиме. Приобретение лицензии (или лицензий)**

   Разные лицензии позволяют использовать разные приложения и службы "Лаборатории Касперского", поэтому вы можете приобрести несколько лицензий.

   Узнайте, какие лицензии вы можете приобрести и минимальное количество устройств для каждой лицензии.

   Kaspersky Security Center Cloud Console входит в состав нескольких решений "Лаборатории Касперского". Выберите, какое решение вы хотите использовать, и приобретите на него лицензию. Вам нужно будет обратиться в "Лабораторию Касперского" или к одному из партнеров "Лаборатории Касперского" с особым запросом, если вы хотите приобрести лицензию на 10 000 и более устройств.

   Используйте таблицу, чтобы проверить какие возможности Системного администрирования доступны в зависимости типа лицензии, по которой используется приложение.

   Если вы хотите использовать Kaspersky Security Center Cloud Console в облачном окружении, таком как Microsoft Azure, прочитайте о вариантах лицензирования для облачных окружений.

   Если вы являетесь поставщиком услуг (MSP), прочтите о лицензировании Kaspersky Security Center Cloud Console для поставщиков услуг.

2. **Активация Kaspersky Security Center Cloud Console при создании рабочей области**

   Вы указываете лицензионный ключ для активации Kaspersky Security Center Cloud Console при создании рабочей области.

   Если у вас несколько лицензионных ключей, укажите любой из них. Позже вам необходимо будет добавить другие лицензионные ключи в Kaspersky Security Center Cloud Console для активации управляемых приложений "Лаборатории Касперского".

3. **Добавление лицензионных ключей для управляемых приложений в хранилище Сервера администрирования**

   Перед развертыванием лицензионных ключей вам нужно добавить эти лицензионные ключи в хранилище Сервера администрирования.

   Лицензионный ключ, указанный вами при создании рабочей области, автоматически добавляется в хранилище Сервера администрирования.

Если у вас более одного лицензионного ключа, добавьте лицензионные ключи по одному в хранилище Сервера администрирования Kaspersky Security Center Cloud Console.

4. **Распространение лицензионных ключей для управляемых приложений**

   Выберите способ распространения лицензионного ключа (или лицензионных ключей) на все устройства, которые вы хотите защитить:

   - Автоматическое распространение

     > Если вы используете разные управляемые приложения и вам важно распространить определенный код активации приложений, используйте другие способы распространения кода активации.

     Kaspersky Security Center позволяет автоматически распространять имеющиеся лицензионные ключи управляемых приложений. Например, в хранилище Сервера администрирования находится три лицензионных ключа. Вам нужно включить параметр **Автоматически распространять лицензионный ключ на управляемые устройства** для всех трех лицензионных ключей. На устройствах организации установлено приложение безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Windows. Обнаружено новое управляемое приложение на устройстве, для которого необходимо распространить лицензионный ключ. Например, приложение определяет, что для этого устройства подходит два лицензионных ключа из хранилища: лицензионный ключ *Ключ_1* и лицензионный ключ *Ключ_2*. Распространяется один из подходящих лицензионных ключей управляемого приложения. В этом случае невозможно предсказать, какой из этих двух лицензионных ключей будет распространен, так как автоматическое распространение лицензионных ключей не предполагает вмешательства администратора.

     При распространении лицензионного ключа на устройства происходит подсчет количества установок для данного лицензионного ключа. Вам необходимо удостовериться, что количество приложений, для которых распространяется лицензионный ключ, не превышает лицензионное ограничение. В случае если количество установок превышает лицензионное ограничение, таким устройствам будет присвоен статус *Критический*.

     Инструкции:

     - Добавление лицензионного ключа в хранилище Сервера администрирования.
     - Автоматическое распространение лицензионного ключа.

   - Распространение с помощью задачи добавления лицензионного ключа управляемого приложения

     В случае использования задачи добавления лицензионного ключа управляемого приложения вы можете выбрать лицензионный ключ, который необходимо распространить на устройства, и выбрать устройства удобным вам способом, например, выбрав группу администрирования или выборку устройств.

     Инструкции:

     - Добавление лицензионного ключа в хранилище Сервера администрирования.
     - Распространение лицензионного ключа на клиентские устройства.

   - Добавление кода активации или файла ключа вручную на устройства

     Вы можете активировать установленное приложение "Лаборатории Касперского" локально, используя инструменты приложения. Дополнительную информацию см. в документации к установленным приложениям.

5. **Проверка на каких устройствах активированы управляемые приложения "Лаборатории Касперского"**

   Чтобы убедиться, что лицензионные ключи распространены правильно, просмотрите список лицензионных ключей, которые используются для приложения.

6. **Настройка событий, связанных с истечением срока действия лицензии**

   Настройте события, чтобы получать уведомления, когда срок действия ваших лицензионных ключей истек или скоро истекает:

   - Критические события Сервера администрирования
   - События отказа функционирования Сервера администрирования
   - События предупреждения Сервера администрирования
   - Информационные события Сервера администрирования

Использование Kaspersky Marketplace для выбора бизнес-решений

Marketplace – раздел главного меню, позволяющий просмотреть весь спектр бизнес-решений "Лаборатории Касперского", выбрать те, которые вам нужны, и перейти к покупке на сайте "Лаборатории Касперского". Вы можете использовать фильтры для просмотра только тех решений, которые соответствуют вашей организации и требованиям вашей системы информационной безопасности. Когда вы выбираете решение, Kaspersky Next XDR Expert перенаправляет вас на соответствующую страницу на сайте "Лаборатории Касперского", чтобы вы могли узнать о решении подробнее. Каждая веб-страница позволяет вам перейти к покупке или содержит инструкции по процессу покупки.

В разделе **Marketplace** вы можете фильтровать решения "Лаборатории Касперского" по следующим критериям:

- Количество устройств (конечных точек, серверов и других типов активов), которые вы хотите защитить:
  - 50–250
  - 250–1000
  - Более 1000
- Уровень опытности команды информационной безопасности вашей организации:
  - **Foundations**

    Этот уровень типичен для предприятий, в которых есть только ИТ-команда. Максимально возможное количество угроз блокируется автоматически.
  - **Optimum**

    Этот уровень типичен для предприятий, у которых есть конкретная функция ИТ-безопасности в ИТ-команде. На этом уровне компаниям требуются решения, которые позволят им противостоять товарным угрозам и угрозам в обход существующих превентивных механизмов.
  - **Expert**

    Этот уровень типичен для предприятий со сложной и распределенной ИТ-средой. Группа ИТ-безопасности состоит из опытных специалистов, или в компании есть группа SOC (Security Operations Center). Необходимые решения позволяют компаниям противостоять комплексным угрозам и целевым атакам.

- Типы активов, которые вы хотите защитить:
  - **Конечные точки**: рабочие станции сотрудников, физические и виртуальные машины, встраиваемые системы.
  - **Серверы**: физические и виртуальные серверы.
  - **Cloud**: публичные, частные или гибридные облачные среды; облачные сервисы.
  - **Сеть**: локальная сеть, ИТ-инфраструктура.
  - **Услуга**: услуги, связанные с безопасностью, предоставляемые "Лабораторией Касперского".

Чтобы найти и приобрести бизнес-решение "Лабораторией Касперского":

1. В главном окне приложения перейдите в раздел **Marketplace**.

   По умолчанию в разделе отображаются все доступные бизнес-решения "Лаборатории Касперского".

2. Чтобы просмотреть только те решения, которые подходят вашей организации, выберите нужные значения в фильтрах.

3. Нажмите на решение, которое вы хотите приобрести или о котором хотите узнать больше.

Вы будете перенаправлены на веб-страницу решения. Следуйте инструкциям на экране, чтобы перейти к покупке.

Лицензии и минимальное количество устройств для каждой лицензии

Если вы хотите использовать коммерческую версию приложения Kaspersky Security Center Cloud Console, перед созданием первой рабочей области вам нужно приобрести лицензию. В таблице ниже показаны лицензии, которые вы можете приобрести, и минимальное количество устройств для каждой лицензии (даже если вы хотите защитить меньшее количество устройств):

Лицензии, которые позволяют использовать Kaspersky Security Center Cloud Console

Лицензия	Минимальное количество устройств (даже если вы хотите защитить меньшее количество устройств)
Kaspersky Endpoint Security для бизнеса Стандартный	Для коммерческих лицензий: 300 Для коммерческих лицензий (по подписке): 100
Kaspersky Endpoint Security для бизнеса Расширенный	Для коммерческих лицензий: 300 Для коммерческих лицензий (по подписке): 100
Kaspersky Total Security для бизнеса.	300
Kaspersky Endpoint Detection and Response Optimum	Для коммерческих лицензий: 300 Для коммерческих лицензий (по подписке): 100
Kaspersky Endpoint Detection and Response Expert	50
Kaspersky Security для виртуальных и облачных сред, настольный компьютер	Для коммерческих лицензий: 300 Для коммерческих лицензий (по подписке): 100.
Kaspersky Security для виртуальных и облачных сред, сервер	50
Kaspersky Security для виртуальных и облачных сред, ядро	20
Kaspersky Security для виртуальных и облачных сред, процессор	20

Лицензия	Минимальное количество устройств (даже если вы хотите защитить меньшее количество устройств)
Kaspersky Security для виртуальных и облачных сред Enterprise, настольный компьютер	Для коммерческих лицензий: 300 Для коммерческих лицензий (по подписке): 100.
Kaspersky Security для виртуальных и облачных сред Enterprise, сервер	50
Kaspersky Security для виртуальных и облачных сред Enterprise, процессор	20
Kaspersky Embedded Systems Security	300
Kaspersky Embedded Systems Security Compliance Edition	300
Kaspersky Symphony (в настоящее время доступно только в России)	300
Kaspersky Next EDR Foundations	100 пользователей. Каждая лицензия может применяться к одному устройству PC/Mac и к двум мобильным устройствам.
Kaspersky Next EDR Optimum	100 пользователей. Каждая лицензия может применяться к одному устройству PC/Mac и к двум мобильным устройствам.
Kaspersky Next Complete Security	100 пользователей. Каждая лицензия может применяться к одному устройству PC/Mac и к двум мобильным устройствам.
Kaspersky Next EDR Expert	100 пользователей. Каждая лицензия может применяться к одному устройству PC/Mac и к двум мобильным устройствам.
Kaspersky Symphony XDR	100 пользователей. Каждая лицензия может применяться к одному устройству PC/Mac и к двум мобильным устройствам.
Kaspersky Next MXDR Optimum	150 пользователей.
Kaspersky XDR Optimum (в настоящее время доступно только в России и СНГ)	Для коммерческих лицензий: 300 пользователей. Для коммерческих лицензий (по подписке): 100 пользователей.
Kaspersky Security для бизнеса Профессиональный	100 пользователей. Каждая лицензия может применяться к одному устройству PC/Mac и к двум мобильным устройствам.

Если вы хотите защитить более 10 000 устройств, вам нужно отправить запрос в Службу технической поддержки "Лаборатории Касперского" и указать информацию о рабочей области, которую вы хотите создать.

События превышения лицензионного ограничения

Kaspersky Security Center Cloud Console позволяет получать информацию о событиях превышения лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах.

Уровень важности событий о превышении лицензионного ограничения определяется по следующим правилам:

- Если количество используемых лицензионных единиц одной лицензии лежит в интервале 90–100% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Информационное сообщение**.
- Если количество используемых лицензионных единиц одной лицензии лежит в интервале 100–110% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Предупреждение**.
- Если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Критическое событие**.

Способы распространения кодов активации на управляемые устройства

Приложения "Лаборатории Касперского" установленные на управляемых устройствах, должны быть активированы путем применения кода активации к каждой из приложений. Вы не можете использовать файлы ключей для лицензирования управляемых приложений; вы можете применять только коды активации. Код активации может быть распространен следующими способами:

- автоматическое распространение;
- с помощью задачи добавления лицензионного ключа управляемого приложения;
- активация управляемого приложения вручную.

Приложения "Лаборатории Касперского" могут использовать одновременно несколько лицензионных ключей. Например, Kaspersky Endpoint Security для Windows может использовать два лицензионных ключа: один для Kaspersky Endpoint Security для Windows и один для активации встроенных функций Endpoint Detection and Response.

Кроме того, приложения "Лаборатории Касперского" могут иметь не только активный лицензионный ключ, но и резервный лицензионный ключ. Приложение "Лаборатории Касперского" использует активный в данный момент ключ и сохраняет резервный ключ, который будет применяться после истечения срока действия активного ключа. Вы можете добавить активный или резервный лицензионный ключ любым из перечисленных выше способов. Приложение, для которого вы добавляете лицензионный ключ, определяет, является ли ключ активным или резервным. Определение ключа не зависит от способа, который вы используете для добавления лицензионного ключа.

Добавление лицензионного ключа Сервера администрирования

Чтобы добавить лицензионный ключ Сервера администрирования:

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Перейдите в раздел **Лицензионные ключи** и нажмите на кнопку **Выбрать** в одном из следующих разделов:

   - **Действующая лицензия**, если вы хотите добавить активный лицензионный ключ.
   - **Резервный лицензионный ключ**, если вы хотите добавить резервный лицензионный ключ.

     Вы можете добавить резервный лицензионный ключ только в том случае, если активный лицензионный ключ уже добавлен.

3. В открывшемся окне выберите необходимый лицензионный ключ из таблицы.

   При необходимости вы можете добавить новый лицензионный ключ, нажав на кнопку **Добавить лицензионный ключ** и указав лицензионный ключ в открывшейся правой панели.

4. Нажмите на кнопку **ОК**.

Окно закроется, лицензионный ключ Сервера администрирования добавлен, информация о лицензионном ключе отобразится в разделе **Лицензионные ключи**.

При необходимости вы можете заменить выбранный лицензионный ключ, нажав на кнопку **Изменить** и указав другой лицензионный ключ. Также вы можете удалить лицензионный ключ.

Добавление лицензионного ключа в хранилище Сервера администрирования

При добавлении лицензионного ключа с помощью Kaspersky Security Center Cloud Console свойства лицензионного ключа сохраняются на Сервере администрирования. На основании этой информации приложение формирует отчет об использовании лицензионных ключей и уведомляет администратора об истечении сроков действия лицензий и о превышении лицензионных ограничений, заложенных в свойствах лицензионных ключей. Вы можете настраивать параметры оповещений об использовании лицензионных ключей в составе параметров Сервера администрирования.

Чтобы добавить лицензионный ключ в хранилище Сервера администрирования:

1. В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии**.
2. Нажмите на кнопку **Добавить**.
3. Укажите код активации в текстовом поле и нажмите на кнопку **Отправить**.
4. Нажмите на кнопку **Закрыть**.

Лицензионный ключ или несколько лицензионных ключей добавлены в хранилище Сервера администрирования.

Распространение лицензионного ключа на клиентские устройства

Kaspersky Security Center Cloud Console позволяет распространить лицензионный ключ на клиентские устройства автоматически или с помощью задачи **Активация приложения**. Вы можете использовать задачу для распространения ключей в определенной группе устройств. При распространении лицензионного ключа с помощью задачи учитывается лицензионное ограничение на количество устройств. Используйте автоматическое распространение ключей, чтобы автоматически прекратить распространение лицензионного ключа при достижении лицензионного ограничения.

Если вы включили автоматическое распространение лицензионного ключа, не создавайте задачу **Активация приложения** для распространения этого ключа на клиентские устройства. Иначе нагрузка на Сервер администрирования увеличится из-за частой синхронизации.

Перед распространением добавьте лицензионный ключ в хранилище Сервера администрирования.

*Чтобы распространить лицензионный ключ на клиентские устройства с помощью задачи **Активация приложения**:*

1. В главном окне приложения перейдите в раздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится **мастер создания задачи**. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В раскрывающемся списке **Приложение** выберите приложение, для которого вы хотите добавить лицензионный ключ.
4. В списке **Тип задачи** выберите задачу **Активация приложения**. В зависимости от приложения задача может также называться **Добавление ключа**.
5. В поле **Название задачи** укажите название новой задачи.
6. Выберите устройства, которым будет назначена задача.
7. На шаге мастера **Выбор лицензионного ключа** перейдите по ссылке **Добавить ключ**, чтобы добавить лицензионный ключ.
8. В панели добавления ключа добавьте лицензионный ключ, используя один из следующих параметров:

   Вам необходимо добавить лицензионный ключ только в том случае, если вы не добавляли его в хранилище Сервера администрирования до создания задачи **Активация приложения**.

   - Выберите параметр **Ввести код активации**, чтобы ввести код активации, а затем выполните следующие действия:

     a. Укажите код активации и нажмите на кнопку **Отправить**.

        Информация о лицензионном ключе отображается в панели добавления ключа.

     b. Нажмите на кнопку **Сохранить**.

Если вы хотите автоматически распространять лицензионный ключ на управляемые устройства, включите параметр **Автоматически распространять лицензионный ключ на управляемые устройства**.

Панель добавления ключа закрыта.

- Выберите параметр **Добавить файл ключа**, чтобы добавить файл ключа, и выполните следующие действия:

  a. Нажмите на кнопку **Выберите файл ключа**.

  b. В открывшемся окне выберите файл ключа и нажмите на кнопку **Открыть**.

  Информация о лицензионном ключе отображается в панели добавления лицензионного ключа.

  c. Нажмите на кнопку **Сохранить**.

  Если вы хотите автоматически распространять лицензионный ключ на управляемые устройства, включите параметр **Автоматически распространять лицензионный ключ на управляемые устройства**.

  Панель добавления ключа закрыта.

9. Выберите лицензионный ключ в таблице ключей.

10. Если вы хотите заменить активный лицензионный ключ, на шаге мастера **Информация о лицензии** снимите флажок **Использовать в качестве резервного лицензионного ключа**.

    Например, это необходимо, когда организация меняется и на устройстве требуется ключ другой организации или если ключ был перевыпущен и срок действия новой лицензии истекает раньше, чем срок действия текущей лицензии. Чтобы избежать ошибок, снимите флажок **Использовать как резервный лицензионный ключ**.

    Если вы хотите узнать больше о проблемах, которые могут возникнуть при добавлении лицензионного ключа в Kaspersky Security Center Cloud Console, и способах их решения, обратитесь к Базе знаний Kaspersky Security Center Cloud Console.

11. Если на шаге мастера **Завершение создания задачи** включить параметр **Открыть окно свойств задачи после ее создания**, вы сможете изменить установленные по умолчанию значения параметров задачи.

    Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже.

12. Нажмите на кнопку **Готово**.

    В результате работы мастера задача создана. Если включен параметр **Открыть окно свойств задачи после ее создания**, автоматически откроется окно параметров задачи. В этом окне вы можете указать общие параметры задачи и изменить параметры, указанные при создании задачи, если это необходимо.

    Вы также можете открыть окно свойств задачи, нажав на название созданной задачи в списке задач.

    Задача будет создана, настроена и отобразится в списке задач.

13. Чтобы запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

    Вы также можете создать расписание запуска задачи на вкладке **Расписание** в окне свойств задачи.

Подробное описание параметров запуска по расписанию см. в общих параметрах задачи.

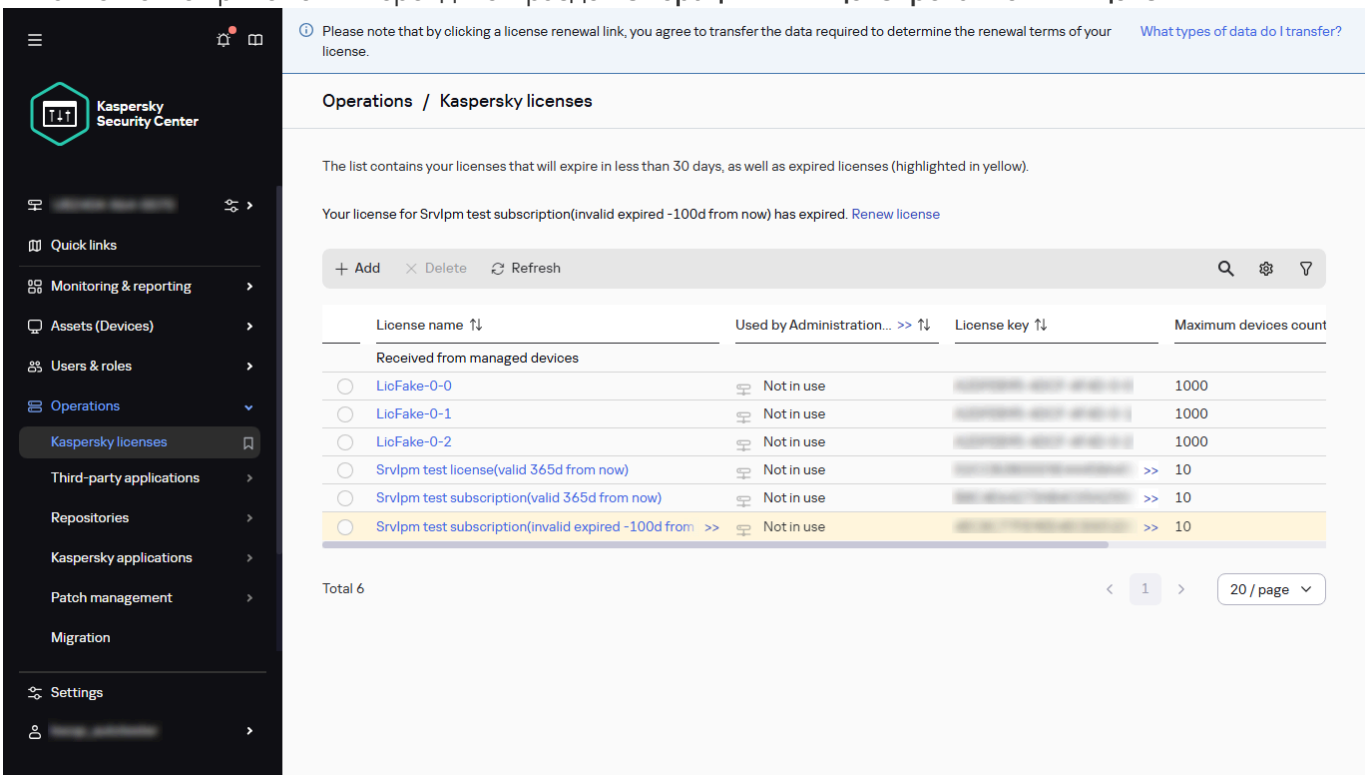
После завершения задачи, лицензионный ключ распространится на выбранные устройства.

Автоматическое распространение лицензионного ключа.

Kaspersky SIEM Cloud позволяет автоматически распространять на управляемые устройства лицензионные ключи, размещенные в хранилище ключей на Сервере администрирования.

Чтобы автоматически распространять лицензионный ключ на управляемые устройства:

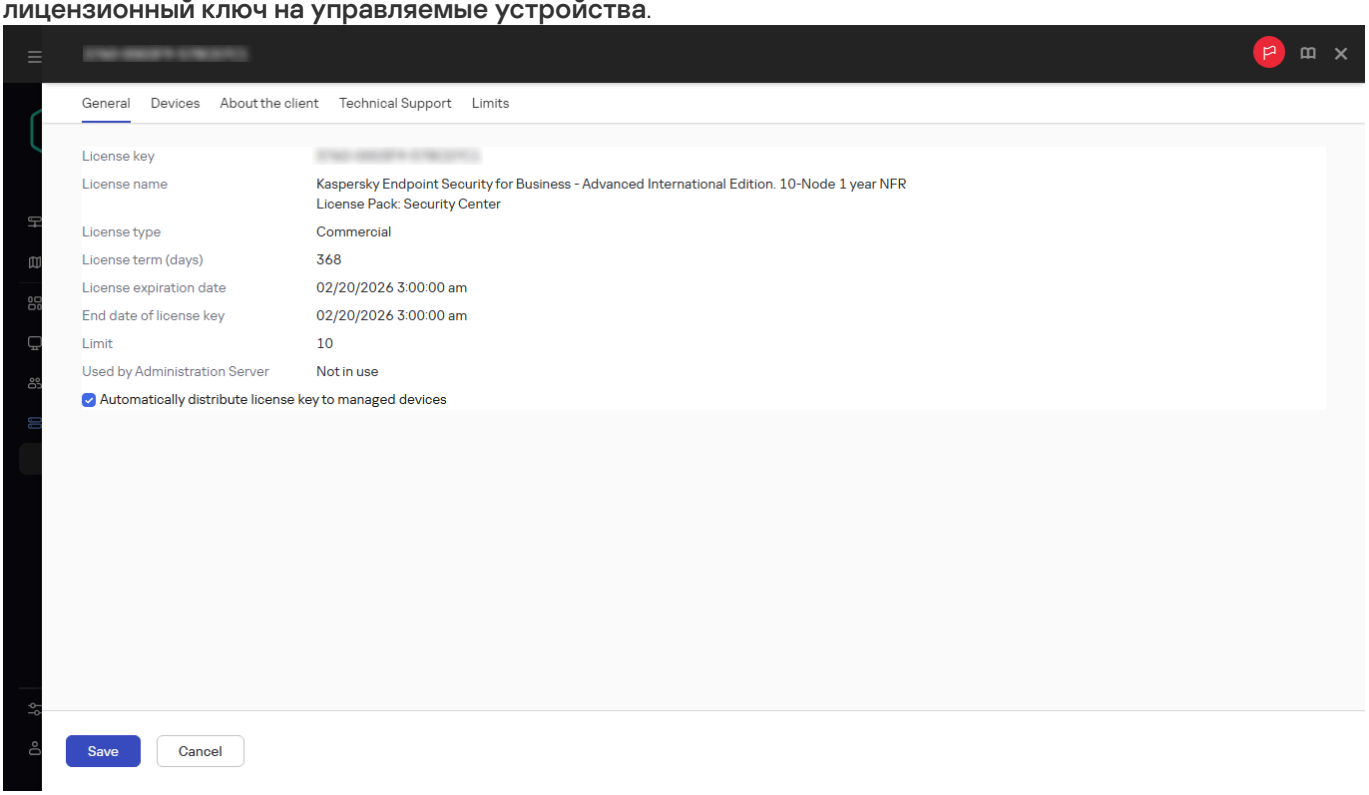
1. В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии**.



Список лицензий

2. Нажмите на имя лицензионного ключа, который вы хотите автоматически распространять на устройства.

3. В открывшемся окне свойств лицензионного ключа установите флажок **Автоматически распространять лицензионный ключ на управляемые устройства**.



Окно свойств лицензионного ключа

4. Нажмите на кнопку **Сохранить**.

Лицензионный ключ будет автоматически распространяться на те устройства, для которых он подходит.

Распространение лицензионного ключа выполняется средствами Агента администрирования. Задачи распространения резервного лицензионного ключа для приложения при этом не создаются.

При автоматическом распространении лицензионного ключа учитывается лицензионное ограничение на количество устройств. Лицензионное ограничение задано в свойствах лицензионного ключа. Если лицензионное ограничение достигнуто, распространение лицензионного ключа на устройства автоматически прекращается.

Обратите внимание, что автоматически распространяемый лицензионный ключ может не отображаться в хранилище виртуального Сервера администрирования в следующих случаях:

- Лицензионный ключ недействителен для приложения.
- Виртуальный Сервер администрирования не имеет управляемых устройств.
- Лицензионный ключ уже используется для устройств, управляемых другим виртуальным Сервером администрирования, и достигнуто лицензионное ограничение на количество устройств.

Виртуальный Сервер администрирования автоматически распространяет лицензионные ключи из своего хранилища и из хранилища Сервера администрирования. Рекомендуется:

- Используйте задачу *Добавить лицензионный ключ*, чтобы выбрать лицензионный ключ, который необходимо развернуть на устройствах.
- Не выключайте параметр **Разрешить автоматическое распространение лицензионных ключей этого виртуального Сервера на его устройства** в параметрах виртуального Сервера администрирования. Иначе виртуальный Сервер администрирования не будет распространять лицензионные ключи на устройства, в том числе лицензионные ключи из хранилища Сервера администрирования.

Если установлен флажок **Автоматически распространять лицензионный ключ на управляемые устройства** в окне свойств лицензионного ключа, лицензионный ключ будет немедленно распространен в вашей сети. Если вы не выберете этот параметр, вы можете использовать задачу распространения лицензионного ключа позже.

Автоматическое распространение лицензионных ключей, настроенных на главном Сервере администрирования, не включает устройства, управляемые невиртуальными подчиненными Серверами администрирования.

Просмотр информации об используемых лицензионных ключах

Чтобы просмотреть список лицензионных ключей, добавленных в хранилище Сервера администрирования:

В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии**.

Отобразится список файлов ключей и кодов активации, добавленных в хранилище Сервера администрирования.

Чтобы просмотреть подробную информацию о лицензионном ключе:

1. В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии**.
2. Нажмите на имя требуемого лицензионного ключа.

В открывшемся окне свойств лицензионного ключа вы можете просмотреть:

- На вкладке **Общие** – основную информацию о лицензионном ключе.
- На вкладке **Устройства** – список клиентских устройств, на которых использовался лицензионный ключ для активации установленного приложения "Лаборатории Касперского".
- На вкладке **Ограничения** – список лицензионных ограничений.

  Если вы активировали Сервер администрирования по лицензии Kaspersky Security для бизнеса Профессиональный, на вкладке **Ограничения** отображается поле **XDR-O** со значением **Включено**.

Чтобы просмотреть, какие лицензионные ключи распространены на выбранное клиентское устройство:

1. В главном окне приложения перейдите в раздел **Управление активами** → **Управляемые устройства**.
2. Нажмите на имя требуемого устройства.

3. В открывшемся окне свойств устройства выберите вкладку **Приложения**.

4. Нажмите на название приложения, для которого вы хотите просмотреть информацию о распространенном лицензионном ключе.

5. В открывшемся окне свойств приложения перейдите на вкладку **Общие** и откройте раздел **Лицензия**.

Отобразится основная информация об активных и резервных лицензионных ключах.

Для определения актуальных параметров лицензионных ключей виртуального Сервера администрирования Сервер администрирования отправляет запрос на серверы активации "Лаборатории Касперского" не реже одного раза в сутки. Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы.

Просмотр информации о лицензионных ключах приложения

Чтобы узнать, какие лицензионные ключи используются приложением "Лаборатории Касперского":

1. В дереве консоли Kaspersky SIEM Cloud выберите узел **Управляемые устройства** и перейдите на вкладку **Устройства**.

2. Откройте контекстное меню требуемого устройства по правой клавише мыши и выберите пункт **Свойства**.

3. В открывшемся окне свойств устройства выберите раздел **Приложения**.

4. В появившемся списке приложений выберите приложение, лицензионные ключи которого вы хотите просмотреть, и нажмите на кнопку **Свойства**.

5. В открывшемся окне свойств Сервера администрирования выберите раздел **Лицензионные ключи**.

   Информация отображается в рабочей области этого раздела.

Удаление лицензионного ключа Сервера администрирования

Чтобы удалить лицензионный ключ Сервера администрирования:

1. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

2. В открывшемся окне свойств Сервера администрирования выберите раздел **Лицензионные ключи**.

3. Удалите лицензионный ключ, нажав на кнопку **Удалить**.

Лицензионный ключ удален.

Если был добавлен резервный лицензионный ключ, резервный лицензионный ключ автоматически становится активным лицензионным ключом после удаления предыдущего активного лицензионного ключа.

После удаления активного лицензионного ключа Сервера администрирования возможности Системного администрирования и Управления мобильными устройствами становятся недоступными. Можно добавить удаленный лицензионный ключ повторно или добавить другой лицензионный ключ.

Удаление лицензионного ключа из хранилища

При удалении активного лицензионного ключа, который распространен на управляемые устройства, приложения продолжают работать на управляемых устройствах.

Чтобы удалить файл ключа или код активации из хранилища Сервера администрирования:

1. Убедитесь, что Сервер администрирования не использует файл ключ или код активации, который вы хотите удалить. Если Сервер администрирования использует такой ключ, вы не сможете удалить ключ. Чтобы выполнить проверку:

   a. В главном окне приложения нажмите на имя Сервера администрирования.

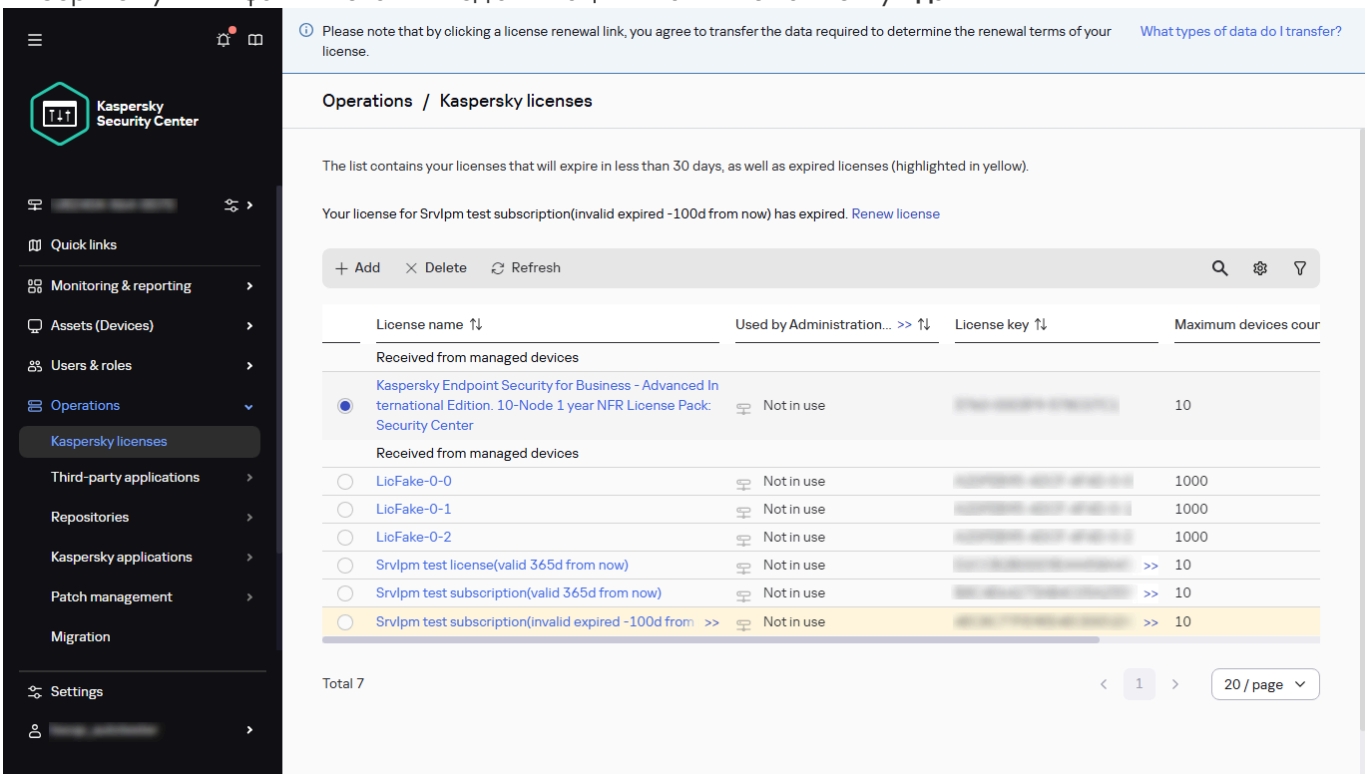
   Откроется окно свойств Сервера администрирования.

   b. На вкладке **Общие** выберите раздел **Лицензионные ключи**.

   c. Если в открывшемся разделе отображается требуемый файл ключ или код активации, нажмите на кнопку **Удалить активный лицензионный ключ** и подтвердите операцию. После этого Сервер администрирования не использует удаленный лицензионный ключ, ключ остается в хранилище Сервера администрирования. Если требуемый файл ключ или код активации не отображается, Сервер администрирования его не использует.

2. В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии**.

3. Выберите нужный файл ключа или код активации и нажмите на кнопку **Удалить**.



Список лицензий

Выбранный файл ключа или код активации удален из хранилища.

Можно добавить удаленный лицензионный ключ повторно или добавить другой лицензионный ключ.

Просмотр списка устройств, на которых приложение "Лаборатории Касперского" не активировано

Вы можете просмотреть список всех устройств, на которых установлено приложение "Лаборатории Касперского", но не активировано (например, лицензия отсутствует или истек срок действия).

Чтобы просмотреть устройства, на которых не активировано приложение "Лаборатории Касперского":

1. В главном окне приложения перейдите в раздел **Задачи**.

   Отобразится список задач.

2. Нажмите на название задачи Обновление, связанной с рассматриваемым приложением "Лаборатории Касперского".

   Окно свойств задачи отображается с несколькими именными вкладками.

3. В окне свойств задачи выберите раздел **Результаты**.

   В столбце **Устройство или подчиненный Сервер** отображаются устройства, на которых задача была выполнена успешно.

4. Сортировать столбец **Устройство или подчиненный Сервер**.

   В столбце **Устройство или подчиненный Сервер** отображаются устройства, на которых задача была выполнена успешно. Устройства, на которых задача не выполнена из-за отсутствия лицензии, являются устройствами, на которых приложение не активировано.

Отзыв согласия с Лицензионным соглашением

Если вы решите прекратить защиту некоторых своих клиентских устройств, вы можете отозвать Лицензионное соглашение для любого управляемого приложения "Лаборатории Касперского". Вам нужно удалить выбранное приложение и его инсталляционный пакет, прежде чем отзывать Лицензионное соглашение этого приложения. Инсталляционные пакеты необходимо удалить с Сервера администрирования и его виртуальных Серверов администрирования.

Лицензионные соглашения, принятые на виртуальном Сервере администрирования, можно отозвать на виртуальном Сервере администрирования или на главном Сервере администрирования. Лицензионные соглашения, принятые на главном Сервере администрирования, можно отозвать только на главном Сервере администрирования.

Чтобы отозвать Лицензионное соглашение для управляемых приложений "Лаборатории Касперского":

1. В главном окне приложения нажмите на имя Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Общие** окна свойств Сервера администрирования выберите раздел **Лицензионные соглашения**.

   Отобразится список Лицензионных соглашений, принятых при создании инсталляционных пакетов или установке обновлений.

3. В списке выберите Лицензионные соглашения, которые вы хотите отозвать.

   Можно просмотреть следующие свойства Лицензионных соглашений:

   - Дата принятия Лицензионного соглашения.
   - Имя пользователя, принявшего Лицензионное соглашение.
   - Можно ли отозвать Лицензионное соглашение.

4. Нажмите на дату принятия любого Лицензионного соглашения, чтобы открыть окно его свойств, в котором отображаются следующие данные:

   - Имя пользователя, принявшего Лицензионное соглашение.
   - Дата принятия Лицензионного соглашения.
   - Уникальный идентификатор (UID) Лицензионного соглашения.
   - Полный текст Лицензионного соглашения.
   - Список объектов (инсталляционных пакетов, обновлений), связанных с Лицензионным соглашением, и их соответствующие имена и типы.

5. В нижней части окна свойств Лицензионного соглашения нажмите на кнопку **Отозвать Лицензионное соглашение**.

   Если выбранное Лицензионное соглашение можно отозвать только путем деинсталляции приложения или если это Лицензионное соглашение можно отозвать только на главном Сервере администрирования, вместо кнопки **Отозвать Лицензионное соглашение** отображается уведомление об этом ограничении.

   > Если существуют какие-либо объекты (инсталляционные пакеты и соответствующие им задачи), которые не позволяют отозвать Лицензионное соглашение, отображается уведомление об этом. Вы не можете продолжить отзыв, пока не удалите эти объекты.

   В открывшемся окне отобразится сообщение о том, что сначала необходимо удалить приложение "Лаборатории Касперского", которому соответствует это Лицензионное соглашение.

6. Нажмите на кнопку, подтверждающую отзыв лицензии.

Лицензионное соглашение отозвано. Лицензионное соглашение больше не отображается в списке Лицензионных соглашений в разделе **Лицензионные соглашения**. Окно свойств Лицензионного соглашения закрывается; приложение больше не установлено.

Продление срока действия лицензии приложений "Лаборатории Касперского"

Вы можете продлить срок действия лицензии приложений "Лаборатории Касперского", срок действия которой истек или скоро истечет (менее чем через 30 дней).

Чтобы продлить срок действия лицензии, который истекает или уже истек:

1. Выполните одно из следующих действий:

   - В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии**.
   - В главном окне приложения перейдите в раздел **Мониторинг** → **Панель мониторинга** и перейдите по ссылке **Просмотреть лицензии, срок действия которых истек** рядом с уведомлением.

   Откроется окно **Лицензии**, в котором вы можете просмотреть и продлить срок действия лицензии.

2. Перейдите по ссылке **Продлить срок действия лицензии** рядом с требуемой лицензией.

   Нажимая на ссылку продления срока действия лицензии, вы соглашаетесь передавать в "Лабораторию Касперского" следующие данные Open Single Management Platform: версию, локализацию, которую вы используете, идентификатор лицензии на программное обеспечение (то есть идентификатор лицензии, которую вы продлеваете), а также то, приобрели ли вы лицензию через компанию-партнера или нет.

3. В открывшемся окне продления срока действия лицензии следуйте инструкциям.

   Срок действия лицензии продлен.

В OSMP Console уведомления отображаются при приближении истечения срока действия лицензии по следующему расписанию:

- за 30 дней до истечения срока действия;
- за 7 дней до истечения срока действия;
- за 3 дней до истечения срока действия;
- за 24 часа до истечения срока действия;
- когда срок действия лицензии истек.

Использование Kaspersky SIEM Cloud после истечения срока действия лицензии

После истечения срока действия лицензии "Лаборатория Касперского" может предоставить вам использование Kaspersky Security Center Cloud Console на 90 дней без ограничений. В этот период Сервер администрирования, Агент администрирования и веб-интерфейс Kaspersky Security Center Cloud Console работают без ограничений. Kaspersky Security Center Cloud Console также отправляет статистику KSN в "Лабораторию Касперского" в соответствии с текущими параметрами KSN. Управляемые приложения работают только с ограниченными функциональными возможностями (подробнее см. в документации к соответствующим приложениям).

Когда срок действия лицензии истекает на 90 дней, Kaspersky Security Center Cloud Console автоматически удаляет вашу рабочую область. Если вы хотите сохранить рабочую область, продлите срок действия хотя бы одной лицензии или добавьте ключ в хранилище.

Определения лицензирования

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием приложений "Лаборатории Касперского", управляемых приложением Kaspersky Security Center Cloud Console.

О лицензии

Лицензия – это ограниченное по времени право на использование Kaspersky SIEM Cloud, предоставляемое вам на условиях заключенного Лицензионного договора (Лицензионного соглашения).

Список доступных функций и срок использования приложения зависят от лицензии, по которой используется приложение.

Предусмотрены следующие типы лицензий:

- *Пробная*

  Бесплатная лицензия, предназначенная для ознакомления с приложением. Пробная лицензия имеет небольшой срок действия.

  По истечении срока действия пробной лицензии Kaspersky SIEM Cloud прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

  Вы можете использовать приложение по пробной лицензии только в течение одного срока пробного использования.

- *Коммерческая*

  Платная лицензия.

  По истечении срока действия коммерческой лицензии приложение прекращает выполнять свои основные функции. Для продолжения работы Kaspersky SIEM Cloud вам нужно продлить срок действия коммерческой лицензии. После истечения срока действия лицензии вы не можете далее использовать приложение и должны удалить его с устройства.

  Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить непрерывность защиты устройства от угроз компьютерной безопасности.

О Лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- идентификатор лицензии или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о приложении, которое можно активировать по предоставляемой лицензии;

- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать приложение по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О лицензионном ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать приложение в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный ключ в приложение одним из следующих способов: применить *файл ключа* или ввести *код активации*. Лицензионный ключ отображается в интерфейсе приложения в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в приложение.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы приложения требуется добавить другой лицензионный ключ.

Лицензионный ключ может быть активным и дополнительным (или резервным).

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы приложения. В качестве активного может быть добавлен лицензионный ключ для пробной или коммерческой лицензии. В приложении не может быть больше одного активного лицензионного ключа.

Дополнительный (или резервный) лицензионный ключ – лицензионный ключ, подтверждающий право на использование приложения, но не используемый в текущий момент. Дополнительный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом. Дополнительный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа.

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии не может быть добавлен в качестве дополнительного лицензионного ключа.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ, активирующий Kaspersky SIEM Cloud. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky SIEM Cloud или после заказа пробной версии Kaspersky SIEM Cloud.

Чтобы активировать приложение с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского". Если доступ к серверам через системный DNS невозможен, приложение использует публичные DNS-серверы.

Если приложение было активировано с помощью кода активации, в некоторых случаях после активации приложение регулярно отправляет запросы на серверы активации "Лаборатории Касперского" для проверки текущего статуса лицензионного ключа. Для отправки запросов необходимо предоставить приложению доступ в интернет.

Если вы потеряли код активации после установки приложения, обратитесь к партнеру "Лаборатории Касперского", у которого вы приобрели лицензию.

Вы не можете использовать файлы ключей для активации управляемых приложений; вы можете применить только коды активации.

О подписке

Подписка на Kaspersky SIEM Cloud – это заказ на использование приложения с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на Kaspersky SIEM Cloud можно зарегистрировать у поставщика услуг (например, у интернет-провайдера). Подписку можно продлевать вручную или в автоматическом режиме, или отказаться от нее.

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky SIEM Cloud после окончания ограниченной подписки ее требуется продлевать. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Если подписка ограничена, по ее истечении может предоставляться льготный период для продления подписки, в течение которого функциональность приложения сохраняется. Наличие и длительность льготного периода определяет поставщик услуг.

Чтобы использовать Kaspersky SIEM Cloud по подписке, требуется применить код активации, предоставленный поставщиком услуг.

Вы можете применить другой код активации для использования Kaspersky SIEM Cloud только после окончания подписки или отказа от нее.

В зависимости от поставщика услуг, наборы возможных действий для управления подпиской могут различаться. Поставщик услуг может не предоставлять льготный период для продления подписки, в течение которого функциональность приложения сохраняется.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky SIEM Cloud.

При использовании приложения по подписке Kaspersky SIEM Cloud автоматически обращается к серверу активации через определенные промежутки времени вплоть до даты окончания подписки. Если доступ к серверу через системный DNS невозможен, приложение использует публичные DNS-серверы. Вы можете продлить подписку на веб-сайте поставщика услуг.

Информация о стороннем коде

Информация о стороннем коде содержится в следующих файлах:

- legal_notices_ksccc.txt;
- legal_notices_kuma.txt;
- legal_notices_osmp.txt.

Файл legal_notices.txt также находится в папке установки управляемых приложений.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Flash, PostScript являются либо зарегистрированными товарными знаками, либо товарными знаками компании Adobe в США и/или других странах.

AMD, AMD64 – товарные знаки или зарегистрированные товарные знаки Advanced Micro Devices, Inc.

Amazon, Amazon EC2, Amazon Web Services, AWS и AWS Marketplace являются товарными знаками Amazon.com, Inc. или аффилированных лиц компании.

Apache и Apache Cassandra являются либо зарегистрированными товарными знаками, либо товарными знаками Apache Software Foundation в Соединенных Штатах и/или других странах.

Apple, App Store, AppleScript, Carbon, FileVault, iPhone, Mac, Mac OS, macOS, OS X, Safari, QuickTime – товарные знаки Apple Inc.

Arm – зарегистрированный товарный знак Arm Limited (или дочерних компаний) в США и/или других странах.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

LTS и Ubuntu являются зарегистрированными товарными знаками Canonical Ltd.

Check Point NGFW – товарный знак или зарегистрированный товарный знак Check Point Software Technologies Ltd. или аффилированных компаний.

Cisco, IOS и Snort являются зарегистрированными товарными знаками или товарными знаками Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Citrix, XenServer являются зарегистрированными товарными знаками или товарными знаками Cloud Software Group, Inc. и/или дочерних компаний в США и/или других странах.

Citrix NetScaler является зарегистрированным товарным знаком или товарным знаком компании Cloud Software Group, Inc. и/или ее дочерних компаний в США и/или других странах.

Cloudflare, логотип Cloudflare и Cloudflare Workers являются товарными знаками и/или зарегистрированными товарными знаками компании Cloudflare, Inc. в США и других юрисдикциях.

Словесный знак Grafana и логотип Grafana являются зарегистрированными товарными знаками/знаками обслуживания или товарными знаками/знаками обслуживания Coding Instinct AB в США и других странах и используются с разрешения Coding Instinct. Мы не являемся аффилированной, поддерживаемой или спонсируемой со стороны Coding Instinct или сообщества Grafana компанией.

CorelDRAW – товарный знак или зарегистрированный в Канаде, США и/или других странах товарный знак Corel Corporation и/или ее дочерних компаний.

Dell Technologies и другие товарные знаки являются товарными знаками компании Dell Inc или её дочерних компаний.

Docker и логотип Docker являются товарными знаками или зарегистрированными товарными знаками компании Docker, Inc. в США и/или других странах. Docker, Inc. и другие стороны могут также иметь права на товарные знаки, описанные другими терминами, используемыми в настоящем документе.

Elasticsearch – зарегистрированный в США и других странах товарный знак Elasticsearch BV.

ESET является товарным знаком или зарегистрированным товарным знаком ESET spol. s r.o. или соответствующей компании ESET.

F5 – товарный знак F5 Networks, Inc. в США и в некоторых других странах.

Firebird – зарегистрированный товарный знак Firebird Foundation.

Fortinet, FortiGate, FortiMail, FortiSOAR – товарные знаки или зарегистрированные в США и/или других странах товарные знаки Fortinet, Inc.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

Google, Android, Chrome, Dalvik, Firebase, Google Chrome, Google Maps, Google Play, Google Public DNS – товарные знаки Google LLC.

HUAWEI, EulerOS, Huawei Eudemon являются товарными знаками Huawei Technologies Co., Ltd.

ViPNet является зарегистрированным товарным знаком компании "ИнфоТеКС".

IBM, Guardium, InfoSphere, QRadar – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Intel, Insider являются товарными знаками Intel Corporation или ее дочерних компаний.

Node.js – товарный знак Joyent, Inc.

Juniper, Juniper Networks и JUNOS – товарные знаки или зарегистрированные в США и других странах товарные знаки Juniper Networks, Inc.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Kubernetes является зарегистрированным товарным знаком The Linux Foundation в США и других странах.

Microsoft, Access, Active Directory, ActiveSync, ActiveX, Azure, BitLocker, Excel, Halo, Hyper-V, InfoPath, Internet Explorer, Lync, Microsoft 365, Microsoft Edge, MS-DOS, MultiPoint, Office 365, OneNote, Outlook, PowerPoint, PowerShell, Segoe, SharePoint, Skype, SQL Server, Tahoma, Visio, Win32, Windows, Windows Media, Windows Mobile, Windows Phone, Windows PowerShell, Windows Server и Windows Vista являются товарными знаками группы компаний Microsoft.

CVE – зарегистрированный товарный знак MITRE Corporation.

Mozilla, Firefox являются товарными знаками Mozilla Foundation в США и других странах.

NetApp – товарный знак или зарегистрированный в США и/или других странах товарный знак NetApp, Inc.

Netskope, логотип Netskope и другие названия продуктов Netskope, упомянутые в настоящем документе, являются товарными знаками Netskope, Inc. и/или одной из ее дочерних компаний и могут быть зарегистрированы в Ведомстве по патентам и товарным знакам США и в других странах.

NetWare – товарный знак Novell Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

Novell – товарный знак Novell Enterprises Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

OpenSSL является товарным знаком правообладателя OpenSSL Software Foundation.

Oracle, Java и JavaScript – зарегистрированные товарные знаки компании Oracle и/или аффилированных компаний.

OpenVPN – зарегистрированный товарный знак OpenVPN, Inc.

Parallels, логотип Parallels и Coherence являются товарными знаками или зарегистрированными товарными знаками Parallels International GmbH.

PROOFPOINT является товарным знаком Proofpoint, Inc. в США и других странах.

Chef – товарный знак или зарегистрированный в США и/или других странах товарный знак Progress Software Corporation и/или одной из дочерних или аффилированных компаний.

Puppet – товарный знак или зарегистрированный товарный знак Puppet, Inc.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Ansible является зарегистрированным товарным знаком Red Hat, Inc. в США и других странах.

Red Hat, CentOS, Fedora, Red Hat Enterprise Linux – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

Товарный знак BlackBerry принадлежит Research In Motion Limited, зарегистрирован в США и может быть подан на регистрацию или зарегистрирован в других странах.

Samsung – товарный знак компании SAMSUNG в США или других странах.

Sendmail и другие наименования и названия продуктов – товарные знаки или зарегистрированные товарные знаки Sendmail, Inc.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

SolarWinds, Dameware – товарные знаки, права на которые принадлежат компании SolarWinds Worldwide, LLC или аффилированным лицам компании, зарегистрированы в Бюро по патентам и товарным знакам США, а также могут быть зарегистрированы или находиться в процессе регистрации в других странах.

Splunk – товарный знак и зарегистрированный в США и других странах товарный знак Splunk, Inc.

Название CommuniGate Pro – товарный знак или зарегистрированный товарный знак Stalker Software, Inc.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

Symantec – товарный знак или зарегистрированный в США и других странах товарный знак Symantec Corporation или аффилированных компаний.

Владельцем товарного знака Symbian является Symbian Foundation Ltd.

OpenAPI – товарный знак компании The Linux Foundation.

Rocky Linux является товарным знаком The Rocky Enterprise Software Foundation.

Trend Micro является товарным знаком или зарегистрированным товарным знаком Trend Micro Incorporated.

Наименования, изображения и логотипы, идентифицирующие продукты и услуги UserGate, являются фирменными знаками UserGate и/или ее дочерних компаний или филиалов, а сами продукты являются собственностью UserGate.

VMware, VMware ESXi, VMware Horizon, VMware vCenter, VMware vSphere, VMware Workstation, Carbon Black – зарегистрированные товарные знаки и/или товарные знаки VMware, Inc. в США и других странах.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

ClickHouse является зарегистрированным товарным знаком ClickHouse, Inc. https://clickhouse.com/

Zabbix – зарегистрированный товарный знак Zabbix SIA.

The MITRE Corporation Terms of Use

LICENSE

The MITRE Corporation (MITRE) hereby grants you a non-exclusive, royalty-free license to use ATT&CK® for research, development, and commercial purposes. Any copy you make for such purposes is authorized provided that you reproduce MITRE's copyright designation and this license in any such copy.

"© 2025 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation."

DISCLAIMERS

MITRE does not claim ATT&CK enumerates all possibilities for the types of actions and behaviors documented as part of its adversary model and framework of techniques. Using the information contained within ATT&CK to address or cover full categories of techniques will not guarantee full defensive coverage as there may be undisclosed techniques or variations on existing techniques not documented by ATT&CK.

ALL DOCUMENTS AND THE INFORMATION CONTAINED THEREIN ARE PROVIDED ON AN "AS IS" BASIS AND THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE MITRE CORPORATION, ITS BOARD OF TRUSTEES, OFFICERS, AGENTS, AND EMPLOYEES, DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION THEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.