kaspersky

Kaspersky CyberTrace

© 2026 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky CyberTrace

О Kaspersky CyberTrace

- О потоках данных об угрозах и сертификатах
  - О потоках данных об угрозах Kaspersky Threat Data Feeds
  - О потоках данных об угрозах «OSINT feeds»
  - О сертификатах
- Комплект поставки
- Аппаратные и программные требования

Предоставление данных

Что нового

Руководства по установке и интеграции

- Обзор установки и интеграции
- Руководство по выбору аппаратной конфигурации
  - Рекомендуемые конфигурации в зависимости от режима
    - О тестовом наборе
    - Рекомендации для режима оценки
    - Рекомендации для режима обработки событий на основе TCP
    - Рекомендации для режима обработки индикаторов на основе API
  - Требования к процессору
  - Сетевые требования
  - Требования к памяти
  - Требования к диску
  - Рекомендации по настройке Kaspersky CyberTrace
- Часть 1. Установка Kaspersky CyberTrace
  - Установка в ОС Linux
  - Установка в ОС Windows
  - Первоначальная настройка (мастер первоначальной настройки)
    - Шаг 1. Страница приветствия
    - Шаг 2. Положение о Kaspersky Security Network (KSN)
    - Шаг 3. Настройка прокси-сервера
    - Шаг 4. Настройка лицензирования
    - Шаг 5. Настройки службы
    - Шаг 6. Настройка управления данными
    - Шаг 7. Настройка сертификата
    - Шаг 8. Настройка потоков данных об угрозах
    - Шаг 9. Первоначальная настройка завершена
  - Настройка Kaspersky Endpoint Security

Часть 2. Интеграция Kaspersky CyberTrace с источником событий
Интеграция с Kaspersky Unified Monitoring and Analysis Platform
Интеграция со Splunk
Общие схемы интеграции (Splunk)
Однокомпонентная схема интеграции (Splunk)
Об однокомпонентной схеме интеграции
Шаг 1. Установка Kaspersky CyberTrace (однокомпонентное развертывание)
Шаг 2 (необязательный). Настройка приложения Kaspersky CyberTrace App (однокомпонентное развертывание)
Шаг 3 (необязательный). Настройка скрипта поиска (однокомпонентное развертывание)
Шаг 4. Проверка работоспособности (Splunk, однокомпонентная схема интеграции)
Распределенная схема интеграции (Splunk)
О распределенной схеме интеграции
Шаг 1. Установка приложений Forwarder App и Search Head App
Шаг 2. Настройка Forwarder App и Search Head App (распределенное развертывание)
Шаг 3 (необязательный). Настройка скрипта поиска (распределенное развертывание)
Шаг 4. Проверка работоспособности (Splunk, распределенная интеграция)
Интеграция с ArcSight ESM
Общие сведения об интеграции (ArcSight)
Предварительные условия (ArcSight)
Установка ArcSight SmartConnector (Linux)
Установка ArcSight SmartConnector с помощью консоли (Linux)
Установка ArcSight SmartConnector (Windows)
Стандартная интеграция (ArcSight)
Схемы интеграции (ArcSight)
Шаг 1. Импорт пакета ARB
Шаг 2. Установка ArcSight Forwarding Connector
Шаг 2 (альтернативный). Установка ArcSight Forwarding Connector с помощью консоли
Шаг 3. Настройка Kaspersky CyberTrace для взаимодействия с ArcSight
Шаг 4. Проверка работоспособности (ArcSight)
Указание собственного пользователя ArcSight в настройках ArcSight Forwarding Connector
Интеграция с QRadar
Стандартная интеграция (QRadar)
О стандартной схеме интеграции (QRadar)
Шаг 1. Настройка QRadar для получения последних обновлений
Шаг 2. Отправка набора событий в QRadar
Шаг 3. Пересылка событий из QRadar в Kaspersky CyberTrace Service
Шаг 4. Проверка работоспособности (QRadar)
Шаг 5. Получение свойств пользовательского события
Шаг 6. Создание поискового фильтра для событий Kaspersky CyberTrace
Шаг 7 (необязательный). Отображение событий на информационной панели
Шаг 8 (необязательный). Создание уведомлений о входящих служебных событиях
Шаг 9 (необязательный). Включение индексов добавленных свойств пользовательского события
Альтернативная интеграция (QRadar)
Интеграция с QRadar в случае, если QRadar не может получать обновления
Импорт QID в QRadar
Добавление Kaspersky CyberTrace Service в качестве источника журналов

Сопоставление событий с QID
Указание типа источника журналов
Интеграция с RSA NetWitness
RSA NetWitness
Предварительные условия (RSA NetWitness)
Проверка настройки программного обеспечения (RSA NetWitness)
Стандартная интеграция (RSA NetWitness)
О стандартной схеме интеграции (RSA NetWitness)
Шаг 1. Пересылка событий из RSA NetWitness
Шаг 2. Отправка событий из Kaspersky CyberTrace Service в RSA NetWitness
Шаг 3 (необязательный). Импорт метагруппы для просмотра полей, заполненных Kaspersky CyberTrace Service
Шаг 4 (необязательный). Импорт правил Kaspersky CyberTrace Service в RSA NetWitness
Шаг 5 (необязательный). Импорт предварительно настроенного отчета в RSA NetWitness
Шаг 6 (необязательный). Импорт предварительно настроенных диаграмм и информационной панели в RSA NetWitness
Шаг 7. Проверка работоспособности (RSA NetWitness)
Интеграция с LogRhythm
Шаг 1. Добавление пользовательского типа источника журналов
Шаг 2. Импорт правил и событий Kaspersky CyberTrace
Шаг 3 (необязательный). Добавление событий Kaspersky CyberTrace
Шаг 4 (необязательный). Добавление правил Kaspersky CyberTrace
Шаг 5. Добавление политики Kaspersky CyberTrace
Шаг 6. Добавление источника журналов в System Monitor Agent
Шаг 7. Настройка пересылки журналов в Kaspersky CyberTrace
Шаг 8. Проверка работоспособности
Шаг 9 (необязательный). Создание информационных сообщений о входящих служебных событиях Kaspersky CyberTrace
Шаг 10 (необязательный). Отображение служебных оповещений в LogRhythm
Интеграция с McAfee Enterprise Security Manager
Настройка Kaspersky CyberTrace для интеграции с McAfee Enterprise Security Manager
Пересылка событий из McAfee Enterprise Security Manager в Kaspersky CyberTrace
Парсинг служебных событий Kaspersky CyberTrace в McAfee Enterprise Security Manager
Парсинг событий обнаружения Kaspersky CyberTrace в McAfee Enterprise Security Manager
Просмотр событий Kaspersky CyberTrace в McAfee Enterprise Security Manager
Интеграция с AlienVault USM / OSSIM
Шаги интеграции с AlienVault USM / OSSIM
Настройка Kaspersky CyberTrace для интеграции с AlienVault USM / OSSIM
Пересылка событий из AlienVault USM / OSSIM в Kaspersky CyberTrace
Импорт файлов конфигурации в AlienVault USM / OSSIM
Просмотр событий Kaspersky CyberTrace в AlienVault USM / OSSIM
Интеграция с FortiSIEM
Шаги интеграции с FortiSIEM
Настройка Kaspersky CyberTrace для интеграции с FortiSIEM
Настройка пересылки событий из FortiSIEM

Получение событий из Kaspersky CyberTrace в FortiSIEM
Добавление Kaspersky CyberTrace в качестве источника событий в FortiSIEM
Добавление полей в FortiSIEM
Добавление правил парсинга событий из Kaspersky CyberTrace в FortiSIEM
Добавление описаний событий в FortiSIEM
Отображение полей контекста в FortiSIEM
Поиск событий, полученных из Kaspersky CyberTrace, в FortiSIEM
Интеграция с другими решениями SIEM и не SIEM
Проверка работоспособности (другие SIEM-системы и не-SIEM-системы)
Дополнительные сценарии установки (с использованием DMZ)
Раздельная установка Kaspersky CyberTrace Service и Feed Utility (Windows, сценарий DMZ)
Установка Kaspersky CyberTrace Service и Feed Utility (сценарий DMZ)
Изменение параметров потоков данных об угрозах после установки Kaspersky CyberTrace Service и Feed Utility на разных хостах (сценарий DMZ)
Синхронизация каталогов, содержащих потоки данных об угрозах (сценарий DMZ)
Обновление Kaspersky CyberTrace с предыдущей версии (сценарий DMZ)
Раздельная установка Kaspersky CyberTrace Service и Feed Utility (Linux, сценарий DMZ)
Установка Kaspersky CyberTrace Service и Feed Utility (сценарий DMZ)
Изменение параметров потоков данных об угрозах после установки Kaspersky CyberTrace Service и Feed Utility на разных хостах (сценарий DMZ)
Синхронизация каталогов, содержащих потоки данных об угрозах (сценарий DMZ)
Обновление Kaspersky CyberTrace с предыдущей версии (сценарий DMZ)
Веб-интерфейс Kaspersky CyberTrace
О ролях пользователей
Права доступа в режиме управления данными
Краткое руководство по использованию Kaspersky CyberTrace
Вход в веб-интерфейс Kaspersky CyberTrace
Настройка Kaspersky CyberTrace
Использование распространенных сценариев Kaspersky CyberTrace
Распространенные сценарии работы с потоками данных
Добавление источников событий и проверка входящих событий
Просмотр статистики Kaspersky CyberTrace на информационной панели
Распространенные сценарии работы с индикаторами
Распространенные сценарии работы с обнаружениями киберугроз
Создание регулярного пользовательского отчета по статистике
Руководства пользователя
Использование веб-интерфейса Kaspersky CyberTrace
Вход в веб-интерфейс Kaspersky CyberTrace
Просмотр статистики на информационной панели
Настройка информационной панели
Виджет Обзор статистики
Виджет «Топ обнаруженных индикаторов»
Виджет «Статистика сопоставлений»
Виджет «Статистика по потокам индикаторов»
Виджет «Пересечения потоков индикаторов»
Добавление пользовательских виджетов
Скачивание статистического отчета

Поиск индикаторов
О синтаксисе поиска индикаторов
Об истории поисковых запросов
Поиск по отдельному индикатору
Поиск индикаторов в файлах журналов
Поиск хешей файлов
Просмотр результатов ретроспективного сканирования
Просмотр обнаруженных киберугроз
О категориях обнаружений киберугроз
Экспорт обнаружений киберугроз в файл CSV
Копирование данных обнаружения киберугрозы в буфер обмена
Об обнаружениях ретроспективного сканирования
Работа с индикаторами
Просмотр индикаторов
Добавление индикаторов в список пользовательских сведений о киберугрозах
Проверка индикаторов IP, HASH, MD5, SHA1 и SHA256
Удаление индикаторов
Поиск индикаторов в таблице индикаторов
Управление поисковыми запросами
Просмотр подробной информации об индикаторах
Обогащение индикаторов из внешних источников
Управление доступом к Kaspersky Threat Intelligence Portal (Kaspersky TIP)
Создание доступа к Kaspersky TIP
Просмотр созданных доступов к Kaspersky TIP
Изменение доступа к Kaspersky TIP
Удаление доступа к Kaspersky TIP
Просмотр обогащения индикаторов
Обогащение индикатора из Kaspersky Threat Intelligence Portal
Управление потоком данных Kaspersky Threat Lookup
Скачивание отчетов из Kaspersky Threat Intelligence Portal
Экспорт индикаторов в CSV
Работа со списком пользовательских сведений о киберугрозах
Экспорт индикаторов в NGFW
Экспорт индикаторов в Check Point NGFW
Экспорт индикаторов в FortiGate NGFW
Экспорт индикаторов в UserGate NGFW
Экспорт индикаторов в Palo Alto NGFW
Экспорт индикаторов в Cisco Firewall Management Center
Экспорт индикаторов в Sophos Firewall
Экспорт индикаторов в Broadcom (Symantec) ProxySG
Экспорт индикаторов в Security Code Continent NGFW
Копирование данных индикаторов в буфер обмена
Правила нормализации URL
Работа с ложными срабатываниями
Отметка индикаторов как ложных срабатываний
Исключение индикаторов из списка ложных срабатываний
Работа с ложными срабатываниями

Просмотр индикаторов и связанных с ними обнаруженных киберугроз, отмеченных как ложные срабатывания, на графе
Фильтрация ложных срабатываний и обнаружений киберугроз
Отображение статистики по ложным срабатываниям на информационной панели
Использование графов
Работа с графами
Об узлах и связях
Работа с узлами и связями
О трансформациях
Выполнение трансформаций
Группы узлов
Фильтрация и поиск
Изменение размера графа и полноэкранный режим
Экспорт информации из графа
Использование тегов
Работа с тегами индикатора
Фильтрация индикаторов по тегам
Просмотр задач
Приложение для Splunk
О приложении Kaspersky CyberTrace App для Splunk
Информационная панель Kaspersky CyberTrace Matches
Информационная панель Kaspersky CyberTrace Status
Indicators lookup
Шаблоны информационных сообщений
Создание уведомлений о входящих служебных событиях
Работа с событиями в ArcSight
Информационные панели
Активные каналы
Фильтрация событий для пересылки из ArcSight
Создание уведомлений о входящих служебных событиях
Работа с событиями в RSA NetWitness
Просмотр событий Kaspersky CyberTrace Service
Создание и просмотр отчетов
Создание и просмотр информационных сообщений
Создание информационной панели
Создание уведомлений о входящих служебных событиях
Об информационной панели Kaspersky CyberTrace
Руководство по Log Scanner
Параметры командной строки
Примеры сценариев использования
Конфигурационный файл (Log Scanner)
Рекомендации по использованию Log Scanner
Руководства администратора
Работа с веб-интерфейсом Kaspersky CyberTrace
Работа с предустановленной учетной записью
Уведомления веб-интерфейса Kaspersky CyberTrace

Управление Kaspersky CyberTrace
- Настройки службы
- Настройка служебных оповещений
  - О шаблонах формата служебных оповещений
  - Служебные оповещения, отправляемые Kaspersky CyberTrace
- Пользовательские настройки
  - Работа с локальными учетными записями
  - Настройка аутентификации LDAP
- Настройка тенантов
- Настройка потока данных
  - О потоках данных «Лаборатории Касперского», пользовательских и сторонних потоках данных
  - Импорт сертификата для Kaspersky Threat Data Feeds
  - Указание периода обновления потоков данных об угрозах по умолчанию
  - Использование прокси-сервера для обновления потоков данных
  - Включение и отключение потоков данных об угрозах
  - Выбор доступных полей для потока данных об угрозах
  - Указание правил фильтрации для потока данных об угрозах
  - Сокращение потока данных об угрозах
  - Указание срока хранения записей потока данных об угрозах
  - Запуск обновления потоков данных об угрозах вручную
  - Добавление пользовательского или стороннего потока данных об угрозах
  - Добавление пользовательского или стороннего потока данных об угрозах типа «электронная почта»
  - Настройка пользовательского или стороннего потока данных об угрозах
- Настройка экспорта индикаторов
- Настройка обнаружения киберугроз
- Работа с тегами
- Настройка ретроспективного сканирования
- Управление задачами отчетов для передачи отчетов по статистике
  - Настройка почтового клиента
  - Создание задачи рассылки отчета
  - Запуск, редактирование и удаление задачи отчета
  - Скачивание отчета
- Безопасность
  - Включение и выключение аудита действий пользователей
  - Настройка аудита действий пользователей
  - Скачивание журнала аудита действий пользователей
  - О журнале аудита действий пользователей
    - Формат событий действий пользователей
    - Общие ключи всех событий действий пользователей
    - Класс событий User
    - Класс событий Service
    - Класс событий ServiceSettings
    - Класс событий License
    - Класс событий ServiceFeeds
    - Класс событий Tenant
    - Класс событий TenantSettings
    - Класс событий TenantFeeds

Класс событий TenantIndicators
Класс событий RetroScan
Класс событий ExternalSources
Класс событий IndicatorsExport
Класс событий Reporting
Настройка журналов
Настройка лицензирования
О лицензировании
Ограничения, накладываемые лицензионными ключами
Добавление лицензионного ключа
Удаление лицензионного ключа
Обновление информации о лицензионном ключе
Работа с тенантами
Общая настройка тенанта
Настройка служебных оповещений тенанта
Служебные оповещения, отправляемые для тенанта
Настройка потоков данных тенанта
Настройка источников событий тенанта
Настройка правил нормализации
О регулярных выражениях
Настройка источников событий с помощью пользовательских регулярных выражений
Регулярные выражения для популярных источников событий
Настройка оповещений об обнаружении индикаторов компрометации для тенанта
Настройка формата оповещений об обнаружении индикаторов компрометации
Настройка правил фильтрации для оповещений об обнаружении индикаторов компрометации
О критериях фильтрации оповещений, отправляемых в SIEM-систему
Настройка контекста оповещений об обнаружении индикаторов компрометации
О шаблонах формата служебных оповещений
Настройка отчетов для тенанта
Руководство по Kaspersky CyberTrace Service
О Kaspersky CyberTrace Service
Управление Kaspersky CyberTrace Service
Управление Kaspersky CyberTrace Service посредством systemd (Linux)
Управление Kaspersky CyberTrace Service посредством SCM (Windows)
Справка по конфигурационному файлу Kaspersky CyberTrace Service
О конфигурационном файле (Kaspersky CyberTrace Service)
EULA
IndicatorDatabaseSettings
RetroScan
Detections
LookupSettings
RegExps
RegExps > Source
Feeds
Feed

- ServiceSettings
  - FeedUtil
    - BasesSettings
    - ScanSettings
    - Security
    - CustomFeedsSecurity
    - HTTPServer
  - Audit
- AuthenticationServers
  - AuthenticationServers > AuthenticationServer
- NotificationSettings
  - EventSettings
  - ServiceAlertsSettings
  - AuditAlertsSettings
- Domains
  - Domain
  - InputSettings
    - RegExps
    - Source
    - Source > NormalizingRules
    - Source > Regular expression
    - ConnectionString
    - EventDelimiter
  - OutputSettings
    - EventSettings
    - EventSettings > SendEventFilters
  - Domain > Feeds > Feed
  - ActionableFields
- IoCExports
  - IoCExport
  - IoCExport > Filter
- GraphSettings
- Plugins
  - Plugin

- Включение инкрементных потоков данных об угрозах
- Журнал Kaspersky CyberTrace Service
- О повторной отправке оповещений об обнаружении индикаторов компрометации
- Kaspersky CyberTrace Service в режиме ReplyBack mode
- Особенности обработки событий в Kaspersky CyberTrace Service
- Ограничения на входящие события Kaspersky CyberTrace Service
- Расширение категорий обнаруженных киберугроз

Руководство по Feed Utility

- Работа с потоками данных об угрозах
  - Параметры командной строки Feed Utility
  - Настройка Feed Utility
    - О конфигурационном файле (Feed Utility)
    - Параметры настройки Feed Utility

Правила потоков данных об угрозах
Правила фильтрации
Правила парсинга
Коды возврата Feed Utility
Использование Kaspersky CyberTrace в режиме высокой доступности
О Balancer
Развертывание Balancer
Проверка HTTPS-сертификатов
Настройка экземпляров Kaspersky CyberTrace
Лицензирование
Настройка Balancer
Управление Balancer
Управление Balancer посредством systemd (Linux)
Управление Balancer посредством Диспетчера управления службами (Windows)
Журнал Balancer
Использование Password Utility
Выбор оптимальных потоков данных об угрозах для определенных условий работы
Обновление и управление установкой
Управление установкой в ОС Linux
Управление установкой в ОС Windows
Обновление предыдущей версии Kaspersky CyberTrace
О процессе обновления
Автоматическое обновление в ОС Linux
Автоматическое обновление в ОС Windows
Изменения после обновления
Обновление интеграции Kaspersky CyberTrace (QRadar)
Обновление интеграции Kaspersky CyberTrace (Splunk)
Обновление интеграции Kaspersky CyberTrace (ArcSight)
Обновление интеграции Kaspersky CyberTrace (RSA)
Обновление интеграции Kaspersky CyberTrace (LogRhythm)
Удаление Kaspersky CyberTrace
Удаление Kaspersky CyberTrace (Windows)
Удаление Kaspersky CyberTrace (Linux)
Удаление объектов Kaspersky CyberTrace (QRadar)
Удаление объектов Kaspersky CyberTrace (Splunk)
Удаление объектов Kaspersky CyberTrace (ArcSight)
Удаление объектов Kaspersky CyberTrace (RSA NetWitness)
Добавление самоподписанных SSL-сертификатов для веб-интерфейса Kaspersky CyberTrace
Повторное создание SSL-сертификатов и добавление доверенных сертификатов для веб-интерфейса Kaspersky CyberTrace
Добавление самоподписанного сертификата в браузер как доверенного
Токен доступа для Kaspersky Threat Intelligence Portal
Токен доступа для плагина VirusTotal
Проверка соединения с Kaspersky CyberTrace Service и наличия потоков данных об угрозах
Руководства для разработчиков
Учебное руководство по разработке приложения на Python: часть 1
Учебное руководство по разработке приложения на Python: часть 2

Справочник по REST API
- О REST API
- Доступ к REST API
- Статусы ответов
- Запросы
  - POST lookup
  - POST lookup (режим мультитенантности)
  - GET suppliers
  - POST suppliers
  - GET suppliers/{supplier}
  - GET suppliers/{supplier} (режим мультитенантности)
  - PUT suppliers/{supplier}
  - PUT suppliers/{supplier} (режим мультитенантности)
  - DELETE suppliers/{supplier}
  - PUT suppliers/{supplier}/indicators
  - PUT suppliers/{supplier}/indicators (режим мультитенантности)
  - DELETE suppliers/{supplier}/indicators
  - DELETE suppliers/{supplier}/indicators (режим мультитенантности)
  - GET tags
  - POST tags
  - GET tags/{tag}
  - PUT tags/{tag}
  - DELETE tags/{tag}
  - PUT publicAPI
  - GET publicAPI

Устранение неполадок
- Устранение общих неполадок
- Устранение неполадок Feed Utility
- Устранение неполадок веб-интерфейса Kaspersky CyberTrace
- Устранение неполадок Splunk
- Устранение неполадок ArcSight
- Устранение неполадок QRadar
- Устранение неполадок RSA NetWitness

Рекомендации по снижению рисков безопасности

Обращение в Службу технической поддержки

Информация о стороннем коде

Уведомления о товарных знаках

Справка Kaspersky CyberTrace

Введение в Kaspersky CyberTrace

- О Kaspersky CyberTrace
- Что нового
- Поток данных «Лаборатории Касперского» об угрозах

Начало работы

- Аппаратные и программные требования
- Руководство по выбору аппаратной конфигурации
- Установка в ОС Linux
- Установка в ОС Windows
- Первоначальная настройка
- Интеграция с источником событий

Веб-интерфейс

- Веб-интерфейс Kaspersky CyberTrace
- Работа с веб-интерфейсом Kaspersky CyberTrace

Дополнительные возможности

- Ретроспективное сканирование
- Графы
- Теги
- Тенанты
- Статистика
- REST API

О Kaspersky CyberTrace

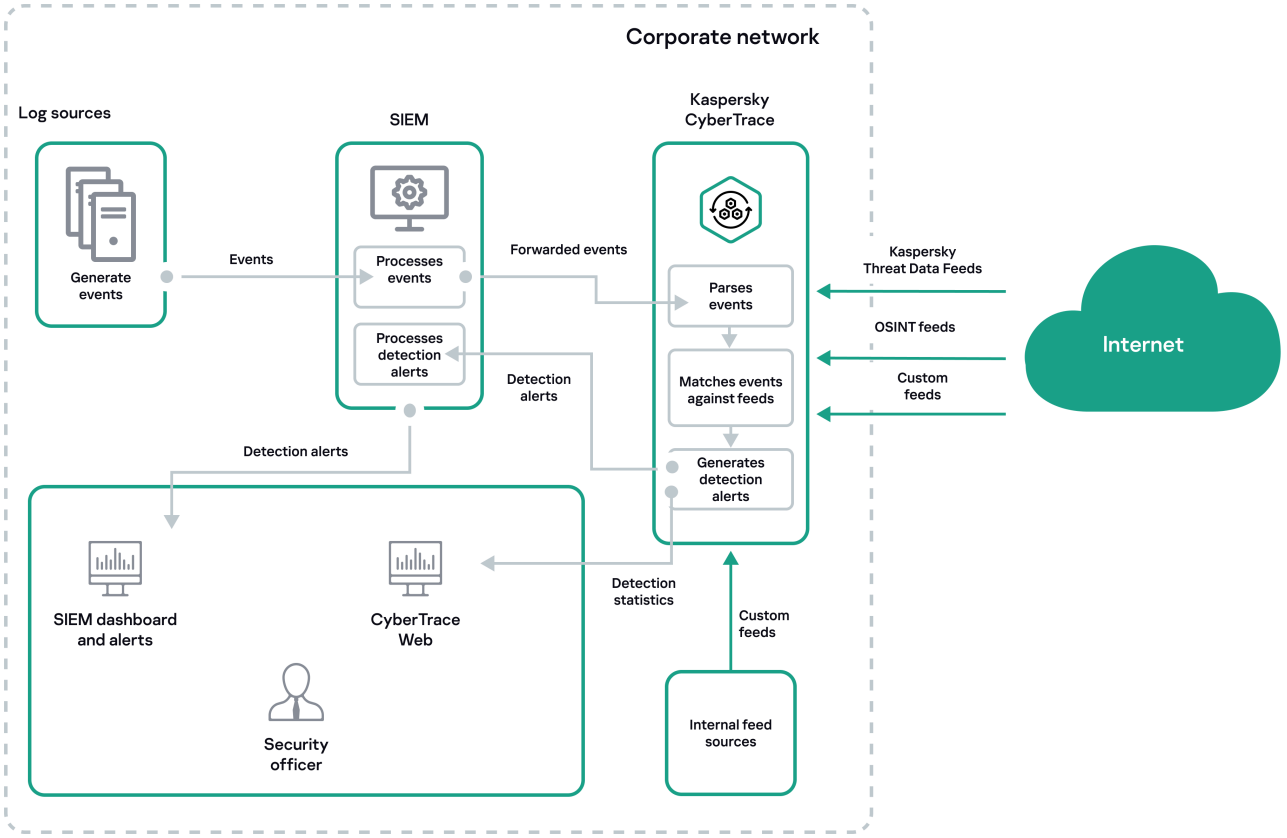
Добро пожаловать в документацию Kaspersky CyberTrace.

Что такое Kaspersky CyberTrace

Kaspersky CyberTrace — это платформа анализа киберугроз (Threat Intelligence Platform), обеспечивающая агрегацию индикаторов компрометации из различных источников, в том числе из потоков данных об угрозах «Лаборатории Касперского», и интеграцию с SIEM-системами (Security Information and Event Management) для автоматического поиска индикаторов компрометации (IoC) в журналах событий безопасности и формирования уведомлений об инцидентах в рамках существующих процессов центра информационной безопасности организации.

Kaspersky CyberTrace использует регулярно обновляемые потоки данных об угрозах для актуализации используемой базы индикаторов компрометации с целью обнаружения киберугроз в журналах событий безопасности и информирования специалистов безопасности о рисках, связанных с той или иной угрозой.

Kaspersky CyberTrace поддерживает интеграцию с источниками данных об угрозах (потоки данных об угрозах от Kaspersky и других поставщиков, OSINT или пользовательские источники), SIEM-системами и источниками журналов событий безопасности. В случае обнаружения IoC в журналах событий безопасности Kaspersky CyberTrace автоматически отправляет в SIEM сообщение об обнаруженном индикаторе, вместе с дополнительной контекстной информацией. Платформа Kaspersky CyberTrace предоставляет аналитикам набор инструментов для классификации оповещений и приоритизации реагирования на них посредством категоризации и дедупликации.



Kaspersky CyberTrace внутри корпоративной сети

Функциональные возможности Kaspersky CyberTrace:

- Автоматическое высокопроизводительное сопоставление входящих журналов и событий безопасности с потоками данных об угрозах Kaspersky Threat Data Feeds, потоками данных OSINT feed или любыми другими пользовательскими потоками данных об угрозах в наиболее популярных форматах (JSON, STIX™, XML, CSV, MISP). Демонстрационные потоки данных об угрозах от Kaspersky и OSINT доступны по умолчанию.

- Внутренний процесс парсинга и сопоставления входящих событий с IoC на стороне Kaspersky CyberTrace значительно снижает нагрузку на SIEM-систему. Kaspersky CyberTrace выполняет парсинг входящих журналов и событий, сопоставляет полученные данные с потоками данных об угрозах и генерирует оповещения при обнаружении киберугроз. Таким образом, на стороне SIEM-системы осуществляется обработка существенно меньшего объема данных.

- Генерируется статистика использования потоков данных об угрозах, что позволяет измерять их эффективность.

- Исследование угроз с помощью поиска конкретных индикаторов (хешей, IP-адресов, доменов, URL) по требованию, а также возможность ручной загрузки журнала событий безопасности с целью генерации отчета об обнаруженных IoC.

- Универсальный подход к интеграции возможностей сопоставления угроз с SIEM-системами и другими средствами контроля безопасности. Коннекторы SIEM для широкого спектра SIEM-систем позволяют визуализировать данные об обнаруженных киберугрозах и эффективно управлять ими.

- Данные об IoC вместе с контекстной информацией хранятся в оперативной памяти для быстрого доступа и фильтрации.

- Веб-интерфейс Kaspersky CyberTrace обеспечивает визуализацию данных, возможности поиска IoC по требованию и доступ к настройке Kaspersky CyberTrace. Веб-интерфейс Kaspersky CyberTrace также поддерживает управление потоками данных об угрозах, правилами парсинга журналов, пользовательскими сведениями о киберугрозах и списками ложных срабатываний, а также источниками событий.

- Интерфейс командной строки для платформ Windows и Linux®.

- Расширенная фильтрация потоков данных и событий журнала. Потоки данных можно конвертировать и фильтровать на основе широкого набора критериев, таких как время, популярность, географическое положение и тип угрозы. События журнала можно фильтровать на основе пользовательских условий.

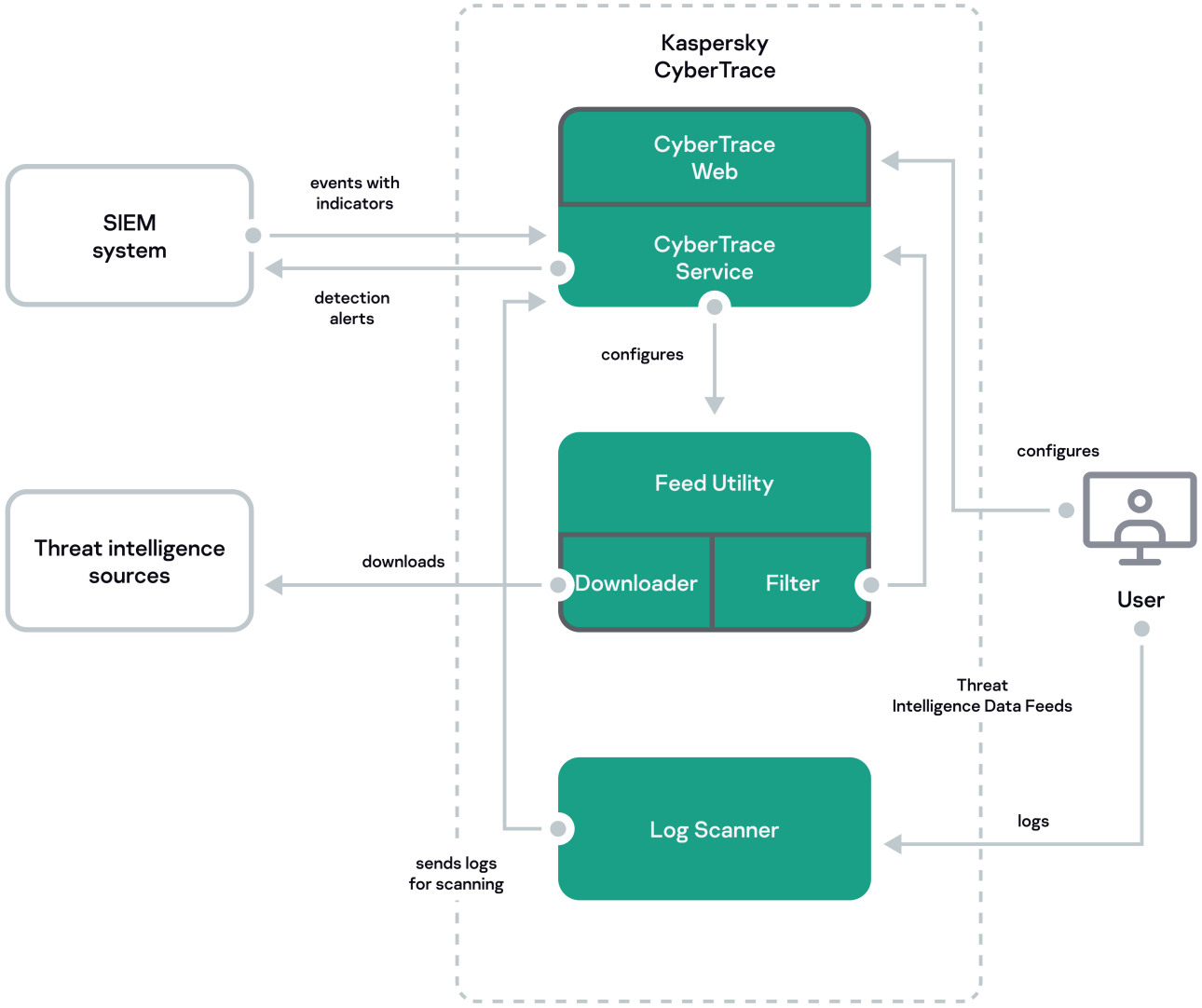
- Поддержка частичного развертывания в демилитаризованной зоне (DMZ). Сервер, на котором выполняется сопоставление данных о событиях с потоками данных об угрозах, может быть изолирован от сети Интернет и получать обновления потоков данных об угрозах от компонента, установленного в DMZ.

- В автономном режиме, когда Kaspersky CyberTrace не интегрируется с SIEM-системами, Kaspersky CyberTrace получает журналы из различных источников, таких как сетевые устройства, обрабатывает эти журналы в соответствии с заданными правилами нормализации и выполняет парсинг журналов в соответствии с заданными регулярными выражениями.

- Результаты поиска, успешно сопоставленные с потоками данных об угрозах, можно экспортировать в формате CSV для интеграции с другими системами (сетевыми экранами, системами обнаружения и предотвращения вторжений (IDS/IPS), пользовательскими инструментами.

- Деобфускация для обнаружения угроз, использующих техники сокрытия вредоносных действий в журналах безопасности.

Основными компонентами Kaspersky CyberTrace являются Kaspersky CyberTrace Service, Feed Utility, Log Scanner и веб-интерфейс Kaspersky CyberTrace.



Основные компоненты Kaspersky CyberTrace

Содержание документации

Эта документация разделена на несколько глав:

- Руководства по установке и интеграции

  В этой главе представлены руководства по установке Kaspersky CyberTrace, интеграции с SIEM-системами и источниками событий, а также по настройке Kaspersky CyberTrace после завершения интеграции.

  > Отправной точкой для процесса установки и интеграции служит раздел Начало работы.

- Руководства пользователя

  В этой главе представлена информация о веб-интерфейсе Kaspersky CyberTrace, а также о приложениях и информационных панелях, обеспечивающих доступ к Kaspersky CyberTrace из SIEM-системы.

- Руководства администратора

  В этой главе представлена информация об управлении Kaspersky CyberTrace, а также рассматриваются расширенные возможности Kaspersky. В этой главе также приводится описание компонентов Kaspersky CyberTrace и рабочих процессов для этих компонентов.

- Устранение неполадок

  В этом разделе представлены решения типичных проблем, которые могут возникать при использовании Kaspersky CyberTrace.

- Рекомендации по снижению рисков безопасности

  В этом разделе приведены рекомендации по снижению потенциальных рисков безопасности при работе с Kaspersky CyberTrace.

О потоках данных об угрозах и сертификатах

В этой главе описываются потоки данных об угрозах и сертификаты, используемые в Kaspersky CyberTrace.

О потоках данных об угрозах Kaspersky Threat Data Feeds

В этом разделе описываются потоки данных об угрозах Kaspersky Threat Data Feeds, доступные для Kaspersky CyberTrace.

Общая информация о Kaspersky Threat Data Feeds

Поставщики средств безопасности базового уровня и организации используют проверенные временем и отлично зарекомендовавшие себя потоки данных об угрозах Kaspersky Threat Data Feeds для создания решений безопасности премиум-класса или для защиты собственного бизнеса.

Кибератаки происходят каждый день. В попытках преодоления средств защиты киберугрозы становятся все более сложными. Злоумышленники используют многоэтапные тщательно подготовленные атаки для нарушения работы организации и/или нанесения вреда клиентам.

«Лаборатория Касперского» поставляет регулярно обновляемые потоки данных об угрозах, содержащих информацию о киберугрозах, а также рисках и последствиях, связанных с ними, помогая более результативно противодействовать злоумышленникам и превентивно защищаться от кибератак.

Информация, содержащаяся в потоках данных об угрозах Kaspersky Threat Data Feeds

Потоки данных об угрозах Kaspersky Threat Data Feeds содержат тщательно проверенные данные об индикаторах угроз, получаемые «Лабораторией Касперского» из многочисленных источников по всему миру в режиме реального времени.

Каждый индикатор в каждом потоке данных об угрозах дополнен контекстом, позволяющим спланировать дальнейшие шаги по расследованию (названия угроз, отметки времени, геолокация, связанные IP-адреса, URL зараженных веб-ресурсов, хеши, популярность и т. д.). Контекстные данные помогают увидеть «общую картину».

Данные в совокупности с контекстом лучше отвечают на вопросы «кто», «что», «где» и «когда», что в конечном счете ведет к полной либо частичной идентификации злоумышленников и помогает принимать своевременные решения и меры, подходящие для конкретной организации.

Доступные группы потоков данных об угрозах

Потоки данных об угрозах Kaspersky Threat Data Feeds, доступные в Kaspersky CyberTrace, можно разделить на следующие основные группы:

- Коммерческие потоки данных об угрозах

  Эта группа содержит обычные коммерческие потоки данных об угрозах, к которым можно получить доступ с коммерческим сертификатом для доступа к потокам данных об угрозах от «Лаборатории Касперского». Потоки данных об угрозах из этой группы охватывают широкий спектр киберугроз.

- Потоки данных об угрозах «APT feeds»

  Потоки данных об угрозах APT feeds — это коммерческие потоки данных о угрозах, которые содержат информацию о киберугрозах, связанных со сложными целевыми атаками (APT).

- Демонстрационные потоки данных об угрозах

  Демонстрационные потоки данных об угрозах можно использовать для ознакомительных целей. Эти потоки данных об угрозах не требуют коммерческого сертификата для доступа к потокам данных об угрозах от «Лаборатории Касперского». Демонстрационные потоки данных об угрозах обеспечивают гораздо более низкий уровень обнаружения киберугроз по сравнению с соответствующими коммерческими версиями.

- Инкрементные потоки данных об угрозах

  Инкрементные потоки данных об угрозах предназначены для уменьшения объема данных, загружаемых с серверов обновлений «Лаборатории Касперского». Инкрементные потоки доступны для самых популярных потоков данных. Для них на серверах обновлений «Лаборатории Касперского» формируются срез данных (полная версия потока данных об угрозах) и инкрементная часть (изменения, применение которых к потоку данных об угрозах приводит его в актуальное состояние). Срез данных генерируется ежедневно, инкрементная часть – в соответствии с частотой обновления потока. Инкрементная часть содержит изменения, применение которых к потоку данных об угрозах приводит его в актуальное состояние. Инкрементная часть генерируется в соответствии с частотой обновления потока данных об угрозах.

Коммерческие потоки данных об угрозах

В этой группе доступны следующие потоки данных об угрозах:

- Botnet C&C URL Data Feed

  Этот поток данных об угрозах содержит URL-адреса и маски для обнаружения серверов управления и контроля (C&C) и веб-ресурсов, связанных с ботнетами.

- Crimeware Hash Data Feed

  Этот поток данных содержит хеши файлов, использованных в мошеннических кампаниях, описанных в отчетах Kaspersky Crimeware.

- Crimeware URL Data Feed

  Этот поток данных содержит информацию об элементах инфраструктуры, связанных с мошенническими кампаниями, описанными в отчетах Kaspersky Crimeware.

- IP Reputation Data Feed

  Этот поток данных содержит IP-адреса, с которых исходит вредоносная активность или которые могут быть использованы для вредоносных действий.

- Malicious Hash Data Feed

  Этот поток данных содержит хеши вредоносных объектов для обнаружения наиболее опасных, распространенных и новых вредоносных программ.

- Malicious URL Data Feed

  Этот поток данных об угрозах содержит вредоносные URL-адреса и маски для обнаружения вредоносных веб-ресурсов.

- Mobile Botnet C&C URL Data Feed

  Этот поток данных об угрозах содержит URL-адреса и маски для обнаружения серверов управления и контроля (C&C) и веб-ресурсов, связанных с мобильными ботнетами.

- Mobile Malicious Hash Data Feed

  Этот поток данных об угрозах содержит хеши вредоносных объектов, нацеленных на мобильные платформы.

- Phishing URL Data Feed

  Этот поток данных содержит фишинговые URL-адреса и маски для обнаружения фишинговых веб-ресурсов.

- Ransomware URL Data Feed

  Этот поток данных об угрозах содержит URL-адреса и маски, к которым пытаются подключиться программы-вымогатели.

- IoT URL Data Feed

  Этот поток данных содержит маски URL, которые ранее использовались для загрузки вредоносных объектов, заражающих устройства IoT (Интернет вещей), такие как IP-камеры, маршрутизаторы и другая техника.

- ICS Hash Data Feed

  Этот поток данных содержит хеши файлов вредоносных объектов, которые используются для атак на инфраструктуру систем управления технологическими процессами (АСУ ТП).

Потоки данных об угрозах «APT feeds»

В этой группе доступны следующие потоки данных об угрозах:

- APT Hash Data Feed

  Этот поток данных содержит хеши вредоносных объектов, которые используются участниками APT-группировок для проведения сложных целевых атак.

- APT IP Data Feed

  Этот поток данных содержит IP-адреса, используемые в кампаниях сложных целевых атак (Advanced Persistent Threat; APT).

- APT URL Data Feed

  Этот поток данных содержит домены, используемые в кампаниях сложных целевых атак (Advanced Persistent Threat; APT).

Демонстрационные потоки данных об угрозах

В этой группе доступны следующие потоки данных об угрозах:

- Demo Botnet C&C URL Data Feed

  Обеспечивает более низкий уровень обнаружения киберугроз по сравнению с Botnet C&C URL Data Feed.

- Demo IP Reputation Data Feed

  Обеспечивает более низкий уровень обнаружения киберугроз по сравнению с IP Reputation Data Feed.

- Demo Malicious Hash Data Feed

  Обеспечивает более низкий уровень обнаружения киберугроз по сравнению с Malicious Hash Data Feed.

- Demo APT URL Data Feed

  — обеспечивает более низкий уровень обнаружения киберугроз по сравнению с APT URL Data Feed.

- Demo APT IP Data Feed

  Обеспечивает более низкий уровень обнаружения киберугроз по сравнению с APT URL Data Feed.

- Demo APT Hash Data Feed

  — обеспечивает более низкий уровень обнаружения киберугроз по сравнению с APT Hash Data Feed.

- Demo Crimeware Hash Data Feed

  Демо-версия Crimeware Hash Data Feed.

- Demo Crimeware URL Data Feed

  Демо-версия Crimeware URL Data Feed.

Инкрементные потоки данных об угрозах

Инкрементные версии доступны для следующих потоков данных об угрозах:

- Botnet C&C URL Data Feed
- Phishing URL Data Feed
- Malicious URL Data Feed

Порядок сортировки записей в потоках данных об угрозах

Записи потока данных об угрозах сортируются следующим образом:

- Записи IP Reputation Data Feed отсортированы по убыванию степени опасности угрозы.
- Записи во всех остальных потоках данных об угрозах отсортированы по убыванию популярности.

О потоках данных об угрозах «OSINT feeds»

В этом разделе описаны потоки данных об угрозах «OSINT feeds», поддерживаемые Kaspersky CyberTrace.

Потоки данных об угрозах OSINT feeds — это общедоступные источники данных об угрозах, предоставляемые организациями и отдельными лицами.

> В комплекте с Kaspersky CyberTrace предоставляется ряд определенных OSINT feed, которые обслуживаются только сторонними организациями. "Лаборатория Касперского" не контролирует эти OSINT feed и, следовательно, не может гарантировать их доступность и качество – эти показатели могут меняться по ходу их работы. Некоторые URL в таблице ниже могут по разным причинам со временем стать неактуальными.

Потоки данных об угрозах OSINT feeds, поддерживаемые Kaspersky CyberTrace

Kaspersky CyberTrace поддерживает потоки данных об угрозах OSINT feeds из следующих источников:

- Abuse.ch

  Этот источник имеет несколько связанных источников информации:

  - Feodo Tracker — это проект abuse.ch, целью которого является распространение информации о C&C-серверах ботнета, связанных с семейством вредоносных программ Feodo (Dridex, Emotet/Heodo).
  - SSLBL — это проект abuse.ch, целью которого является обнаружение вредоносных SSL-соединений путем идентификации SSL-сертификатов, используемых C&C-серверами ботнета, и добавления их в список запрещенных.

- BlockList.de

  Это бесплатная и добровольная услуга, предоставляемая специалистом по мошенничеству/компрометации, чьи серверы часто подвергаются атакам по SSH, Mail Login, FTP, веб-серверу и другим службам.

  BlockList.de содержит информацию о более чем 70 000 атаках за двенадцать часов в режиме реального времени и использует Whois (abuse-mailbox, abuse@, security@, email, remarks), RIPE Abuse Finder и базу данных Abuse Contact Database от abusix.org для обнаружения скомпрометированных адресов, присвоенных атакующим хостам.

- Cyber Crime Tracker

  Cyber Crime Tracker осуществляет мониторинг различных семейств вредоносных программ, которые используются для совершения киберпреступлений, таких как банковские трояны и программы-вымогатели. В его список входят в основном C&C-серверы вредоносных программ, а также файловые хеши Zeus и семейств вредоносных программ, производных от Zeus.

- Proofpoint ET intelligence

  Этот источник предоставляет информацию о возникающих угрозах.

- TORnodes

  Этот источник предоставляет список IP-адресов для узлов TOR.

В следующей таблице перечислены поддерживаемые потоки данных об угрозах «OSINT feeds».

Потоки данных об угрозах «OSINT feeds»

Идентификатор	Описание	Ссылка
Abuse.ch_Feodo_BlockIP	Feodo IP Blocklist	https://feodotracker.abuse.ch/downloads/ipblocklist.csv
Abuse.ch_SSL_Certificate_BlockHash	SSL Certificate Denylist	https://sslbl.abuse.ch/blacklist/sslblacklist.csv
Blocklist.de_BlockIP	Blocklist.de IP Blocklist	https://lists.blocklist.de/lists/all.txt
CyberCrime_Tracker_BlockUrl	Cyber Crime Tracker URL Blocklist	http://cybercrime-tracker.net/all.php
EmergingThreats_BlockIP	Raw IPs for the firewall block lists	https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt
EmergingThreats_CompromisedIP	Compromised IP addresses	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
MalwareBazaar	Список хешей вредоносных объектов MalwareBazaar	https://bazaar.abuse.ch/export/txt/md5/recent/
Выходные узлы Tor	Список IP-адресов выходных узлов сети Tor Существующие ограничения: получение данных из этого источника возможно только раз в 30 минут.	https://www.dan.me.uk/torlist/?exit
URL-адреса вредоносного ПО URLhaus	Список URL-адресов, связанных с распространением вредоносного программного обеспечения	https://urlhaus.abuse.ch/downloads/csv_recent/

О сертификатах

Kaspersky CyberTrace использует TLS сертификат для загрузки потоков данных об угрозах. Сертификат определяет, какие потоки данных об угрозах Kaspersky CyberTrace может загружать с серверов обновлений.

Типы сертификатов

Kaspersky CyberTrace может использовать сертификаты двух типов:

- Демо-сертификат для доступа к потокам данных об угрозах от «Лаборатории Касперского»

  Этот сертификат входит в комплект поставки. Он позволяет получать доступ к демо-версии потоков данных об угрозах Kaspersky Threat Data Feeds.

- Коммерческий сертификат для доступа к потокам данных об угрозах от «Лаборатории Касперского»

  Этот сертификат позволяет получить доступ к одному или нескольким потокам данных об угрозах Kaspersky Threat Data Feeds.

  Чтобы получить коммерческий сертификат для доступа к потокам данных об угрозах от «Лаборатории Касперского», свяжитесь с командой Kaspersky Cybersecurity Service по адресу intelligence@kaspersky.com.

Сертификаты и безопасность

Когда Kaspersky CyberTrace устанавливает соединение с серверами Kaspersky, он передает сертификат в Kaspersky в зашифрованном виде. Соединение между Kaspersky CyberTrace и серверами Kaspersky также зашифровано, чтобы обеспечить защиту всех передаваемый данных.

Комплект поставки

В этом разделе описывается содержимое комплекта поставки Kaspersky CyberTrace.

Типы комплектов поставки

Kaspersky CyberTrace распространяется в комплектах поставки следующих типов:

- В виде пакета RPM и набора дополнительных файлов

  Комплект поставки этого типа предназначен для установки в ОС Linux.

- В виде пакета DEB и набора дополнительных файлов

  Комплект поставки этого типа предназначен для установки в ОС Linux.

- В виде исполняемого файла установщика и набора дополнительных файлов

  Комплект поставки этого типа предназначен для установки в ОС Windows.

О файлах интеграции

Все комплекты поставки Kaspersky CyberTrace настроены для интеграции с конкретным SIEM-системой или для автономной интеграции. Каждый комплект поставки содержит ряд файлов, которые можно использовать для интеграции с данной SIEM-системой. Кроме того, конфигурационные файлы Kaspersky CyberTrace Service и других утилит, содержащихся в комплекте поставки, также настроены для удобства интеграции с соответствующей SIEM-системой.

Например, комплект поставки для Splunk содержит все компоненты Kaspersky CyberTrace и, кроме того, содержит настроенные конфигурационные файлы для Kaspersky CyberTrace Service и Feed Utility, позволяющие работать со Splunk. Каталог integration внутри комплекта поставки содержит приложения для всех вариантов схем интеграции Splunk. Эти приложения можно развернуть и использовать в инфраструктуре Splunk.

Комплекты поставки RPM и DEB

Дистрибутив этого типа содержит следующие файлы и папки.

Состав комплекта поставки (пакет RPM или DEB)

Элемент	Описание
Kaspersky_CyberTrace-Linux-%architecture%-%version%-Release.rpm (пакет RPM) Kaspersky_CyberTrace-Linux-%architecture%-%version%-Release.deb (пакет DEB)	Пакет установки Kaspersky CyberTrace. Список файлов внутри этого пакета приведен в подразделе «Файлы, содержащиеся в архивах и пакетах (Linux)» ниже.
legal_notices.txt	Юридическая информация.
run.sh	Скрипт установки.

Комплект поставки в виде исполняемого файла установщика

В комплект поставки этого типа входит следующий файл.

Состав комплекта поставки (исполняемый файл установщика)

Элемент	Описание
Kaspersky_CyberTrace-Windows-%architecture-version%-Release.exe	Исполняемый файл установщика. Список файлов внутри этого пакета приведен в подразделе «Файлы, содержащиеся в архивах и пакетах (Windows)» ниже.

Файлы, содержащиеся в архивах и пакетах (Linux)

Пакеты RPM и DEB содержат следующий набор файлов. Файлы, содержащиеся в архивах и пакетах (Linux)

Элемент	Описание
bin/.need_run_wizard	Мастер первоначальной настройки Этот файл удаляется после завершения первоначальной настройки.

bin/configure	Бинарный файл утилиты-конфигуратора
bin/en_US/*	Файлы английской локализации.
bin/kl_feed_service	Бинарный файл Kaspersky CyberTrace Service.
bin/kl_balancer_log.conf	Конфигурационный файл журнала Balancer.
bin/kl_feed_service_log.conf	Конфигурационный файл журнала Kaspersky CyberTrace Service.
bin/kl_balancer	Бинарный файл Balancer.
bin/kl_balancer.conf	Конфигурационный файл Balancer
bin/libapp_core_legacy.so	Динамические библиотеки, компоненты и конфигурационные файлы.
bin/libapp_core_meta.so	
bin/libapp_core.so	
bin/libcrypto_components_meta.so	
bin/libcrypto_components.so	
bin/libcrypto_ssl_1_1.so	
bin/libdns_client.so	
bin/libformat_recognizer.so	
bin/libinstrumental_meta.so	
bin/libinstrumental_services.so	
bin/libkey_value_storage.so	
bin/libkl_remote.so	
bin/libkl_service.so	
bin/liblicensing_meta.so	
bin/liblicensing_product_facade.so	
bin/libnetwork_services.so	
bin/libpacked_io.so	
bin/libpersistent_queue.so	
bin/libpr_eka_proxy.so	
bin/libpropmap.so	
bin/libstorage.so	
bin/libtm.so	
bin/libupdater_facade.so	
bin/libupdater_meta.so	
bin/libksn_facade.so	
bin/libksn_meta.so	
bin/loader.so	
bin/pdk.esm	
bin/tm_profile.xml	
modules/elasticsearch/*	Каталог, содержащий файлы базы данных Elasticsearch.
dmz/cron_dmz.sh	Скрипт для обновления потоков данных об угрозах с отдельного компьютера.
dmz/demofeeds.pem	Сертификат необходим для доступа к демонстрационным потокам данных об угрозах.
dmz/feeds.pem	Сертификат необходим для доступа к демонстрационным потокам данных об угрозах. Он заменяется сертификатом, указанным при установке Kaspersky CyberTrace.

dmz/kl_feed_compiler	Бинарный файл, используемый Feed Utility для компиляции потоков данных об угрозах.
dmz/kl_feed_util	Бинарный файл Feed Utility.
dmz/kl_feed_util.conf	Конфигурационный файл Feed Utility.
dmz/TextExtraction	Утилита для парсинга файлов PDF.
doc/Kaspersky_CyberTrace_Online_Documentation.html	HTML-страница, перенаправляющая на онлайн-документацию по Kaspersky CyberTrace.
doc/legal_notices.txt	Юридическая информация.
doc/license.txt	Лицензионное соглашение (EULA).
doc/ReleaseNotes.txt	Заметки о выпуске на английском языке.
doc/ReleaseNotes_ru-RU.txt	Заметки о выпуске на русском языке.
etc/systemd/system/cybertrace.service	Файл модуля systemd для Kaspersky CyberTrace Service.
etc/systemd/system/cybertrace_balancer.service	Файл модуля systemd для Balancer.
etc/systemd/system/cybertrace_db.service	Файл модуля systemd для службы базы данных Elasticsearch.
etc/kl_feed_service.conf	Конфигурационный файл Kaspersky CyberTrace Service.
etc/kl_feed_service_template.conf	Шаблон конфигурационного файла.
etc/kl_feed_util.conf	Конфигурационный файл Feed Utility.
etc/kl_feed_util_diff.conf	Конфигурационный файл Feed Utility для использования с инкрементными потоками данных об угрозах.
feeds/APT_URL_Data_Feed.json.url.bin/* feeds/Botnet_CnC_URL_Data_Feed.json.url.bin/* feeds/IoT_URL_Data_Feed.json.url.bin/* feeds/Malicious_URL_Data_Feed.json.url.bin/* feeds/Mobile_Botnet_CnC_URL_Data_Feed.json.url.bin/* feeds/Phishing_URL_Data_Feed.json.url.bin/* feeds/Ransomware_URL_Data_Feed.json.url.bin/* FalsePositive.json.url.bin/*	Скомпилированные маски URL для потоков данных об угрозах.
feeds/Demo_Botnet_CnC_URL_Data_Feed.json feeds/Demo_IP_Reputation_Data_Feed.json feeds/Demo_Malicious_Hash_Data_Feed.json	Демонстрационные потоки данных об угрозах.
feeds/APT_Hash_Data_Feed.json feeds/APT_IP_Data_Feed.json feeds/APT_URL_Data_Feed.json feeds/Botnet_CnC_URL_Data_Feed.json feeds/ICS_Hash_Data_Feed.json feeds/IoT_URL_Data_Feed.json feeds/IP_Reputation_Data_Feed.json feeds/Malicious_Hash_Data_Feed.json feeds/Malicious_URL_Data_Feed.json feeds/Mobile_Botnet_CnC_URL_Data_Feed.json feeds/Mobile_Malicious_Hash_Data_Feed.json feeds/Phishing_URL_Data_Feed.json feeds/Ransomware_URL_Data_Feed.json	Файлы для проверки работоспособности коммерческих потоков данных об угрозах. При обновлении эти файлы заменяются реальными коммерческими потоками данных.
feeds/FalsePositive.json	Файл потока данных FalsePositive для проверки работоспособности. При обновлении эти файлы заменяются реальными коммерческими потоками данных об угрозах.
httpsrv/etc/kl_feed_info.conf	Файл, содержащий информацию о потоках данных об угрозах Kaspersky Threat Data Feeds.
httpsrv/etc/kl_feed_info_diff.conf	Файл, содержащий информацию о потоках данных об угрозах Kaspersky Threat Data Feeds, для которых доступны инкрементные версии.

httpsrv/etc/ktfsaccess	Файл, содержащий информацию об учетных записях Kaspersky CyberTrace.
httpsrv/etc/ktfsstatistics.kvdb	Вспомогательный файл для веб-интерфейса Kaspersky CyberTrace. Этот файл не входит в комплект поставки, а создается в процессе работы Kaspersky CyberTrace.
httpsrv/etc/ktfsstorage.kvdb	Файл, содержащий информацию об открытых сессиях и выполняющихся задачах. Этот файл не входит в комплект поставки, а создается в дальнейшем в процессе работы Kaspersky CyberTrace.
httpsrv/etc/ktfstasks.kvdb	Вспомогательный файл для веб-интерфейса Kaspersky CyberTrace. Этот файл не входит в комплект поставки, а создается в процессе работы Kaspersky CyberTrace.
httpsrv/etc/osint_feed_list.conf	Файл, содержащий список поддерживаемых потоков данных об угрозах «OSINT feed».
httpsrv/etc/custom_feed_list.conf	Список созданных пользовательских потоков данных. Этот файл не входит в комплект поставки, а создается в процессе работы Kaspersky CyberTrace.
httpsrv/etc/dashboardsinfo.kvdb	Дополнительная информация по виджетам. Этот файл не входит в комплект поставки, а создается в процессе работы Kaspersky CyberTrace.
httpsrv/etc/detected_iocs_statistics.kvdb	Данные виджетов «Топ-N». Этот файл не входит в комплект поставки, а создается в процессе работы Kaspersky CyberTrace.
httpsrv/etc/secure_storage.kvdb	Вспомогательный файл для веб-интерфейса Kaspersky CyberTrace. Этот файл не входит в комплект поставки, а создается в процессе работы Kaspersky CyberTrace.
httpsrv/kl_feed_service_cert.pem	Путь к сертификату в формате PEM на локальном сервере для HTTPS-соединений.
httpsrv/kl_feed_service_private.pem	Путь к закрытому ключу в формате PEM на локальном сервере для HTTPS-соединений.
httpsrv/templates/*	Каталог, содержащий шаблоны для веб-интерфейса Kaspersky CyberTrace.
httpsrv/templates_kuma/*	Каталог, содержащий шаблоны веб-интерфейса Kaspersky CyberTrace для интеграции с KUMA.
integration/*	Файлы для интеграции с конкретной SIEM-системой. Список этих файлов приведен в подразделах «Файлы интеграции...» ниже.
plugins/virus_total/*	Каталог, содержащий файлы для плагина VirusTotal.
scripts/cron_cybertrace.sh	Скрипт для обновления потоков данных об угрозах, когда Kaspersky CyberTrace Service и Feed Utility установлены на разных серверах.
tools/integrity_checker	Утилита, проверяющая подписи плагинов.
tools/kl_access_util	Password Utility
tools/kl_feed_compiler	Бинарный файл, используемый Feed Utility для компиляции потоков данных об угрозах.
tools/kl_feed_util	Бинарный файл Feed Utility.
tools/log_scanner	Бинарный файл Log Scanner.
tools/log_scanner.conf	Конфигурационный файл Log Scanner.
tools/openssl	Бинарный файл OpenSSL.
tools/openssl.cnf	Конфигурационный файл OpenSSL.
tools/output/feeds.info	Вспомогательный файл.
tools/TextExtraction	Утилита для парсинга файлов PDF.
tools/pdf_generator/*	Каталог с утилитой для создания отчетов в формате PDF.
tools/node/*	Каталог с дистрибутивом Nodejs.
var/graphs/*	Каталог с файлами графов.
var/retroscan/*	Каталог с файлами ретроспективного сканирования.
var/ai/*	Каталог с конфигурационными файлами.

var/tzdata/*	Каталог с файлами для настройки часового пояса.
var/updates/*	Каталог с файлами внутренних компонентов Kaspersky CyberTrace.
verification/kl_verification_test_leef.txt	События в формате LEEF для проверки работоспособности.
verification/kl_verification_test_cef.txt	События в формате CEF для проверки работоспособности.
version	Файл с номером версии Kaspersky CyberTrace.

Файлы, содержащиеся в архивах и пакетах (Windows)

Исполняемые файлы установщика содержат следующий набор файлов.

Файлы, содержащиеся в архивах и пакетах (Windows)

Элемент	Описание
bin\. need_run_wizard	Мастер первоначальной настройки Этот файл удаляется после завершения первоначальной настройки.
bin\en_US	Файлы английской локализации.
bin\kl_feed_service.conf	Конфигурационный файл службы <PRODUCT_bin\app_core.dllNAME>.
bin\kl_feed_service.exe	Бинарный файл Kaspersky CyberTrace Service.
bin\kl_balancer_log.conf	Конфигурационный файл журнала Balancer.
bin\kl_feed_service_log.conf	Конфигурационный файл журнала Kaspersky CyberTrace Service.
bin\kl_feed_service_template.conf	Шаблон конфигурационного файла Kaspersky CyberTrace Service.
bin\kl_feed_util.conf	Конфигурационный файл Feed Utility.
bin\kl_balancer.exe	Бинарный файл Balancer.
bin\kl_balancer.conf	Конфигурационный файл Balancer.
bin\kl_feed_util_diff.conf	Конфигурационный файл Feed Utility для использования с инкрементными потоками данных об угрозах.

bin\app_core.dll	Динамические библиотеки, компоненты и конфигурационные файлы.
bin\app_core_etw.dll	
bin\app_core_legacy.dll	
bin\app_core_meta.dll	
bin\concrt140.dll	
bin\crypto_components.dll	
bin\crypto_components_meta.dll	
bin\crypto_ssl_1_1.dll	
bin\dblite.dll	
bin\dns_client.dll	
bin\format_recognizer.dll	
bin\instrumental_meta.dll	
bin\instrumental_services.dll	
bin\key_value_storage.dll	
bin\kl_remote.dll	
bin\kl_service.dll	
bin\licensing_meta.dll	
bin\licensing_product_facade.dll	
bin\msvcp140.dll	
bin\msvcp140_1.dll	
bin\msvcp140_2.dll	
bin\msvcp140_atomic_wait.dll	
bin\msvcp140_codecvt_ids.dll	
bin\network_services.dll	
bin\packed_io.dll	
bin\pdk.esm	
bin\persistent_queue.dll	
bin\prcore.dll	
bin\propmap.dll	
bin\storage.dll	
bin\tm.dll	
bin\updater_facade.dll	
bin\updater_meta.dll	
bin\vcruntime140.dll	
bin\vcruntime140_1.dll	
modules\elasticsearch*	Папка, содержащая файлы базы данных Elasticsearch.
dmz\cron_dmz.cmd	Скрипт обновления потоков данных об угрозах с отдельного сервера.
dmz\demofeeds.pem	Сертификат, необходимый для доступа к демонстрационным потокам данных об угрозах.
dmz\feeds.pem	Сертификат, необходимый для доступа к демонстрационным потокам данных об угрозах. Он заменяется сертификатом, указанным при установке Kaspersky CyberTrace.
dmz\kl_feed_compiler.exe	Бинарный файл, используемый Feed Utility для компиляции потоков данных об угрозах.

dmz\kl_feed_util.conf	Конфигурационный файл Feed Utility.
dmz\kl_feed_util.exe	Бинарный файл Feed Utility.
dmz\TextExtraction.exe	Утилита для парсинга файлов PDF.
doc\Kaspersky_CyberTrace_Online_Documentation.html	HTML-страница, перенаправляющая на онлайн-документацию по Kaspersky CyberTrace.
doc\legal_notices.txt	Юридическая информация.
doc\license.rtf	Лицензионное соглашение (EULA).
doc\ReleaseNotes.txt	Заметки о выпуске на английском языке.
doc\ReleaseNotes_ru-RU.txt	Заметки о выпуске на русском языке.
feeds\APT_URL_Data_Feed.json.url.bin* feeds\Botnet_CnC_URL_Data_Feed.json.url.bin* feeds\IoT_URL_Data_Feed.json.url.bin* feeds\Malicious_URL_Data_Feed.json.url.bin* feeds\Mobile_Botnet_CnC_URL_Data_Feed.json.url.bin* feeds\Phishing_URL_Data_Feed.json.url.bin* feeds\Ransomware_URL_Data_Feed.json.url.bin* feeds\FalsePositive.json.url.bin*	Скомпилированные маски URL для потоков данных об угрозах.
feeds\Demo_Botnet_CnC_URL_Data_Feed.json feeds\Demo_IP_Reputation_Data_Feed.json feeds\Demo_Malicious_Hash_Data_Feed.json	Демонстрационные потоки данных об угрозах.
feeds\APT_Hash_Data_Feed.json feeds\APT_IP_Data_Feed.json feeds\APT_URL_Data_Feed.json feeds\Botnet_CnC_URL_Data_Feed.json feeds\ICS_Hash_Data_Feed.json feeds\IoT_URL_Data_Feed.json feeds\IP_Reputation_Data_Feed.json feeds\Malicious_Hash_Data_Feed.json feeds\Malicious_URL_Data_Feed.json feeds\Mobile_Botnet_CnC_URL_Data_Feed.json feeds\Mobile_Malicious_Hash_Data_Feed.json feeds\Phishing_URL_Data_Feed.json feeds\Ransomware_URL_Data_Feed.json	Файлы для проверки работоспособности коммерческих потоков данных об угрозах. При обновлении эти файлы заменяются реальными коммерческими потоками данных.
feeds\FalsePositive.json	Файл потока данных FalsePositive для проверки работоспособности. При обновлении эти файлы заменяются реальными коммерческими потоками данных об угрозах.
httpsrv\etc\kl_feed_info.conf	Файл, содержащий информацию о потоках данных об угрозах Kaspersky Threat Data Feeds.
httpsrv\etc\kl_feed_info_diff.conf	Файл, содержащий информацию о потоках данных об угрозах Kaspersky Threat Data Feeds, для которых доступны инкрементные версии.
httpsrv\etc\ktfsaccess	Файл, содержащий информацию об учетных записях Kaspersky CyberTrace.
httpsrv\etc\ktfsstatistics.kvdb	Вспомогательный файл для веб-интерфейса Kaspersky CyberTrace. Этот файл не входит в комплект поставки, а создается в процессе работы Kaspersky CyberTrace.
httpsrv\etc\ktfsstorage.kvdb	Файл, содержащий информацию об открытых сессиях и выполняющихся задачах. Этот файл не входит в комплект поставки, а создается в процессе работы Kaspersky CyberTrace.
httpsrv\etc\ktfstasks.kvdb	Вспомогательный файл для веб-интерфейса Kaspersky CyberTrace. Этот файл не входит в комплект поставки, а создается в процессе работы Kaspersky CyberTrace.
httpsrv\etc\osint_feed_list.conf	Файл, содержащий список поддерживаемых потоков данных об угрозах «OSINT feed».

httpsrv\etc\custom_feed_list.conf	Список созданных пользовательских потоков данных. Этот файл не входит в комплект поставки, а создается в процессе работы Kaspersky CyberTrace.
httpsrv\etc\dashboardsinfo.kvdb	Дополнительная информация по виджетам. Этот файл не входит в комплект поставки, а создается в процессе работы Kaspersky CyberTrace.
httpsrv\etc\detected_iocs_statistics.kvdb	Данные виджетов «Топ-N». Этот файл не входит в комплект поставки, а создается в процессе работы Kaspersky CyberTrace.
httpsrv\etc\secure_storage.kvdb	Вспомогательный файл для веб-интерфейса Kaspersky CyberTrace. Этот файл не входит в комплект поставки, а создается в процессе работы Kaspersky CyberTrace.
httpsrv\kl_feed_service_cert.pem	Путь к сертификату в формате PEM на локальном сервере для HTTPS-соединений.
httpsrv\kl_feed_service_private.pem	Путь к закрытому ключу в формате PEM на локальном сервере для HTTPS-соединений.
httpsrv\templates*	Папка, содержащая шаблоны для веб-интерфейса Kaspersky CyberTrace.
httpsrv\templates_kuma	Папка, содержащая шаблоны веб-интерфейса Kaspersky CyberTrace для интеграции с KUMA.
integration*	Файлы для интеграции с конкретной SIEM-системой. Список этих файлов приведен в подразделах «Файлы интеграции...» ниже.
plugins\virus_total*	Папка, содержащая файлы для плагина VirusTotal.
scripts\cron_cybertrace.cmd	Скрипт для обновления потоков данных об угрозах, когда Kaspersky CyberTrace Service и Feed Utility установлены на разных серверах.
tools\integrity_checker.exe	Утилита, проверяющая подписи плагинов.
tools\kl_access_util.exe	Password Utility
tools\kl_feed_compiler.exe	Бинарный файл, используемый Feed Utility для компиляции потоков данных об угрозах.
tools\kl_feed_util.exe	Бинарный файл Feed Utility.
tools\log_scanner.conf	Конфигурационный файл Log Scanner.
tools\log_scanner.exe	Бинарный файл Log Scanner.
tools\openssl.cnf	Конфигурационный файл OpenSSL для генерации самоподписанного сертификата.
tools\openssl.exe	Бинарный файл OpenSSL.
tools\TextExtraction.exe	Утилита для парсинга файлов PDF.
tools\pdf_generator*	Каталог с утилитой для создания отчетов в формате PDF.
tools\node*	Каталог с дистрибутивом Nodejs.
var\graphs*	Папка с файлами графов. Эта папка не входит в комплект поставки и создается при запуске Kaspersky CyberTrace.
var\retroscan*	Папка с файлами ретроспективного сканирования. Эта папка не входит в комплект поставки и создается при запуске Kaspersky CyberTrace.
var\ai*	Каталог с конфигурационными файлами.
var\tzdata*	Каталог с файлами для настройки часового пояса.
var\updates*	Каталог с файлами внутренних компонентов Kaspersky CyberTrace.
verification\kl_verification_test_leef.txt	События в формате LEEF для проверки работоспособности.
verification\kl_verification_test_cef.txt	События в формате CEF для проверки работоспособности.
version	Файл с номером версии Kaspersky CyberTrace.

Файлы интеграции (Splunk)

Файлы интеграции для Splunk описаны в следующей таблице.

Файлы интеграции (Splunk)

Элемент	Описание
/integration/splunk/Kaspersky-CyberTrace-App-for-Splunk.tar.gz	Файл приложения Kaspersky CyberTrace App for Splunk для однокомпонентной схемы интеграции.
/integration/splunk/Kaspersky-CyberTrace-App-for-Splunk_Forwarder.tar.gz	Файл приложения Kaspersky CyberTrace App for Splunk Heavy Forwarder для распределенной схемы интеграции.
/integration/splunk/Kaspersky-CyberTrace-App-for-Splunk_Search-Head.tar.gz	Файл приложения Kaspersky CyberTrace App for Splunk Search Head для распределенной схемы интеграции.
/integration/splunk/Kaspersky-CyberTrace-App-for-Splunk_Universal-Forwarder.tar.gz	Файл приложения Kaspersky CyberTrace App for Splunk Universal Forwarder для распределенной схемы интеграции.

Файлы интеграции (ArcSight)

Файлы интеграции для ArcSight описаны в следующей таблице.

Файлы интеграции (ArcSight)

Элемент	Описание
integration/arcsight/Kaspersky_CyberTrace_Connector.arb	ARB-файл Kaspersky CyberTrace Connector для ArcSight.

Файлы интеграции (QRadar)

Файлы интеграции для QRadar описаны в следующей таблице.

Файлы интеграции (QRadar)

Элемент	Описание
integration/qradar/sample_initiallog.txt	Пример журнала для первой передачи событий в QRadar.
integration/qradar/sample_qid.txt	Пример списка QID для импорта в QRadar.

Файлы интеграции (RSA NetWitness)

Файлы интеграции для RSA NetWitness описаны в следующей таблице.

Файлы интеграции (RSA NetWitness)

Элемент	Описание
integration/rsa/additional_elements/CyberTrace_Charts.zip	Файл, содержащий предварительно настроенные диаграммы.
integration/rsa/additional_elements/CyberTrace_Reports.zip	Файл, содержащий предварительно настроенный отчет.
integration/rsa/additional_elements/CyberTrace_Rules.zip	Файл, содержащий правила для работы с событиями из Kaspersky CyberTrace Service.

integration/rsa/additional_elements/index-concentrator-custom.xml	Пример данных, которые можно добавить в файл index-concentrator-custom.xml. Этот пример данных содержит только описание полей контекста kl.
integration/rsa/additional_elements/Kaspersky CyberTrace.zip	Файл для создания информационной панели Kaspersky CyberTrace в RSA NetWitness 11.0.
integration/rsa/additional_elements/Kaspersky+CyberTrace.cfg	Файл для создания информационной панели Kaspersky CyberTrace в RSA NetWitness 10.6.
integration/rsa/additional_elements/MetaGroups.jsn	Файл, содержащий метагруппу, используемую для просмотра полей в RSA NetWitness, которые заполняет Kaspersky CyberTrace Service.
integration/rsa/additional_elements/MetaGroups_without_kl_fields.jsn	Метагруппа для вкладки «Navigate». Эта метагруппа не содержит полей контекста `kl`.
integration/rsa/additional_elements/table-map-custom.xml	Пример данных, которые можно добавить в файл table-map-custom.xml. Этот пример данных содержит только описание полей контекста `kl`.
integration/rsa/cybertrace/cybertrace.ini	Файл, используемый для интеграции Kaspersky CyberTrace с RSA NetWitness.
integration/rsa/cybertrace/v20_cybertracemsg.xml	Файл, используемый для интеграции Kaspersky CyberTrace с RSA NetWitness

Файлы интеграции (LogRhythm)

Файлы интеграции для LogRhythm описаны в следующей таблице.

Элемент	Описание
integration/logrhythm/events/*	Файлы, содержащие правила Kaspersky CyberTrace для импорта в LogRhythm: • mperule_AbuseCh_Feodo_Block_IP.xml • mperule_AbuseCh_SSL_Certificate_Block_IP.xml • mperule_AbuseCh_SSL_Certificate_Hash_SHA1.xml • mperule_BlocklistDe_Block_IP.xml • mperule_CyberCrime_Tracker_Block_Url.xml • mperule_EmergingThreats_Block_IP.xml • mperule_EmergingThreats_Compromised_IP.xml • mperule_KL_ALERT_ConfigurationUpdated.xml • mperule_KL_ALERT_DetectsStorageExceeded.xml • mperule_KL_ALERT_EPSHardLimit.xml • mperule_KL_ALERT_EPSLimitExceeded.xml • mperule_KL_ALERT_FailedToUpdateFeed.xml • mperule_KL_ALERT_FeedBecameAvailable.xml • mperule_KL_ALERT_FeedBecameUnavailable.xml • mperule_KL_ALERT_FreeSpaceEnds.xml • mperule_KL_ALERT_IndicatorsStoreHardLimit.xml • mperule_KL_ALERT_IndicatorsStoreLimitExceeded.xml • mperule_KL_ALERT_LicenseChanged.xml • mperule_KL_ALERT_LicenseExpired.xml • mperule_KL_ALERT_LicenseExpires.xml • mperule_KL_ALERT_OutdatedFeed.xml • mperule_KL_ALERT_RetroScanCompleted.xml • mperule_KL_ALERT_RetroScanError.xml • mperule_KL_ALERT_RetroScanStorageExceeded.xml • mperule_KL_ALERT_ServiceStarted.xml • mperule_KL_ALERT_ServiceStopped.xml • mperule_KL_ALERT_ServiceUnavailable.xml • mperule_KL_ALERT_UpdatedFeed.xml • mperule_KL_APT_Hash_MD5.xml • mperule_KL_APT_Hash_SHA1.xml • mperule_KL_APT_Hash_SHA256.xml • mperule_KL_APT_IP.xml • mperule_KL_APT_URL.xml • mperule_KL_BotnetCnC_Hash_MD5.xml • mperule_KL_BotnetCnC_Hash_SHA1.xml • mperule_KL_BotnetCnC_Hash_SHA256.xml • mperule_KL_BotnetCnC_URL.xml • mperule_KL_ICS_Hash_MD5.xml • mperule_KL_ICS_Hash_SHA1.xml • mperule_KL_ICS_Hash_SHA256.xml • mperule_KL_InternalTI_Hash_MD5.xml • mperule_KL_InternalTI_Hash_SHA1.xml • mperule_KL_InternalTI_Hash_SHA256.xml • mperule_KL_InternalTI_IP.xml • mperule_KL_InternalTI_URL.xml • mperule_KL_IoT_Hash_MD5.xml • mperule_KL_IoT_Hash_SHA1.xml • mperule_KL_IoT_Hash_SHA256.xml • mperule_KL_IoT_URL.xml • mperule_KL_IP_Reputation.xml • mperule_KL_IP_Reputation_Hash_MD5.xml • mperule_KL_IP_Reputation_Hash_SHA1.xml • mperule_KL_IP_Reputation_Hash_SHA256.xml • mperule_KL_Malicious_Hash_MD5.xml • mperule_KL_Malicious_Hash_SHA1.xml • mperule_KL_Malicious_Hash_SHA256.xml • mperule_KL_Malicious_URL.xml • mperule_KL_Malicious_URL_Hash_MD5.xml • mperule_KL_Malicious_URL_Hash_SHA1.xml • mperule_KL_Malicious_URL_Hash_SHA256.xml • mperule_KL_Mobile_BotnetCnC_Hash_MD5.xml • mperule_KL_Mobile_BotnetCnC_Hash_SHA1.xml • mperule_KL_Mobile_BotnetCnC_Hash_SHA256.xml • mperule_KL_Mobile_BotnetCnC_URL.xml • mperule_KL_Mobile_Malicious_Hash_MD5.xml • mperule_KL_Mobile_Malicious_Hash_SHA1.xml • mperule_KL_Mobile_Malicious_Hash_SHA256.xml • mperule_KL_Phishing_URL.xml • mperule_KL_Ransomware_URL.xml • mperule_KL_Ransomware_URL_Hash_MD5.xml • mperule_KL_Ransomware_URL_Hash_SHA1.xml • mperule_KL_Ransomware_URL_Hash_SHA256.xml

Аппаратные и программные требования

В этой статье указаны версии программ, совместимость Kaspersky CyberTrace с которыми была протестирована и с которыми Kaspersky CyberTrace гарантированно работает корректно. Kaspersky CyberTrace может работать и с другими версиями указанного ниже программного обеспечения, но соответствующие конфигурации не прошли полный цикл тестирования и не включены в список гарантированно поддерживаемых версий.

Kaspersky CyberTrace имеет следующие аппаратные и программные требования:

Поддерживаемые операционные системы

Kaspersky CyberTrace может работать в следующих операционных системах:

- Linux Astra Смоленск 1.8.3.7 (64) (ядро generic)
- РЕД ОС 8
- Debian 12
- Debian 13
- Ubuntu 24.04.2 LTS
- Ubuntu 22.04.4 LTS
- Rocky Linux™ 9.x
- Red Hat® Enterprise Linux® 9.x
- Oracle® Linux® 8.x
- Oracle Linux 9.x
- Microsoft® Windows Server® 2019
- Microsoft Windows Server 2022
- Microsoft Windows Server 2025

Зависимости для Linux

В ОС Linux Kaspersky CyberTrace имеет следующие зависимости:

- Должна быть установлена утилита `less`.

Для создания отчета убедитесь, что в операционной системе Linux установлены следующие библиотеки: glibc версии 2.28, libstdc++ версии 6.0.25.

Программные требования для интеграции с SIEM-системами

При интеграции с SIEM-системами Kaspersky CyberTrace предъявляет следующие требования к программному обеспечению.

Программные требования для интеграции с SIEM-системами

SIEM-система	Программные требования
Splunk	Splunk Enterprise 8.0.0 Более старые версии поддерживаются в Kaspersky CyberTrace 3.1.
ArcSight ESM	ArcSight ESM с 6.8 по 7.0 ArcSight SmartConnector ArcSight Forwarding Connector
QRadar	IBM QRadar v7.2.5
RSA NetWitness	RSA NetWitness® 10.5, 10.6, 11.2 или 11.6.0
LogRhythm	LogRhythm 7.1.7
AlienVault OSSIM	AlienVault OSSIM 5.7.5 Для получения дополнительной информации см. https://support.kaspersky.com/15161.
USM Anywhere	USM Anywhere 5.7.5 Для получения дополнительной информации см. https://support.kaspersky.com/15161.
FortiSIEM	FortiSIEM 5.2 Для получения дополнительной информации см. https://support.kaspersky.com/15146.
Apache Kafka	Apache Kafka 2.4.0 Python 2.7 или 3 Для этой интеграции требуется специальный плагин. Для получения дополнительной информации обращайтесь по адресу intelligence@kaspersky.com.
ArcSight Event Broker	ArcSight Event Broker 2.2 Python 2.7 или 3 Для этой интеграции требуется специальный плагин. Для получения дополнительной информации обращайтесь по адресу intelligence@kaspersky.com.
Elastic Stack (Elasticsearch, Logstash и Kibana)	Logstash 7.2 Java 8 или 11 Для этой интеграции требуется плагин Kaspersky CyberTrace Plug-in for Logstash, который можно скачать бесплатно. Для получения дополнительной информации см. https://support.kaspersky.com/15474.
McAfee ESM	McAfee ESM с 9.6 по 11 Для получения дополнительной информации обращайтесь по адресу intelligence@kaspersky.com.
Kaspersky Unified Monitoring and Analysis Platform (KUMA)	KUMA 4.2

Возможна интеграция и с другими SIEM-системами. Для получения дополнительной информации см. https://support.kaspersky.ru/datafeeds.

Поддерживаемые браузеры

С веб-интерфейсом Kaspersky CyberTrace можно работать в актуальных версиях следующих веб-браузеров:

- Microsoft Edge®
- Mozilla™ Firefox™
- Google Chrome™

Стабильная работа Kaspersky CyberTrace в более ранних версиях перечисленных выше браузеров и в других браузерах не гарантирована.

Требования к процессору

Требования зависят от конкретного варианта использования и используемых потоков данных об угрозах.

Например, при оценке работы Kaspersky CyberTrace по лицензии Community Edition и с включенным ретроспективным сканированием потребуется четырехъядерный процессор.

Дополнительные сведения о требованиях см. в руководстве по выбору аппаратной конфигурации.

Требования к разрешению экрана

Широкоформатный экран, поддерживающий разрешение 1366x768 и выше.

Требования к оперативной памяти и дисковому пространству

Требования зависят от конкретного варианта использования и используемых потоков данных об угрозах.

Например, при оценке работы Kaspersky CyberTrace по лицензии Community Edition и с включенным ретроспективным сканированием потребуется 16 ГБ оперативной памяти и около 470 ГБ свободного места на диске.

Дополнительные сведения о требованиях см. в руководстве по выбору аппаратной конфигурации.

Требования к дисковому пространству можно уменьшить путем отключения сохранения оповещений об обнаружении индикаторов компрометации.

Веб-интерфейс Kaspersky CyberTrace отображает уведомление, когда жесткий диск, на котором установлен Kaspersky CyberTrace, заполняется на 90 процентов. Текст уведомления задается в событии `KL_ALERT_FreeSpaceEnds`. Чтобы изменить это поведение, можно изменить следующие настройки в файле elasticsearch.yml:

- `cluster.routing.allocation.disk.watermark.high` — задает процент использования пространства на жестком диске, при котором выдается уведомление. По умолчанию задано значение 90 процентов.

- `cluster.routing.allocation.disk.watermark.flood_stage` — задает объем пространства на жестком диске (в процентах), который должен быть заполнен, чтобы диск считался полным. `%FreeSpace%` в тексте события `KL_ALERT_FreeSpaceEnds` рассчитывается относительно этого значения. По умолчанию задано значение 95 процентов.

Сетевые требования

Доступ

Сервер, на котором работает Feed Utility, должен иметь доступ к веб-ресурсу https://wlinfo.kaspersky.com/.

Сервер, на котором работает Kaspersky CyberTrace, должен иметь доступ к серверу с SIEM-системой.

Хосты пользователей, работающих с веб-интерфейсом Kaspersky CyberTrace, должны иметь доступ к адресу и порту, используемым веб-интерфейсом Kaspersky CyberTrace.

Если на компьютере включены фильтрация и контроль трафика SSL, необходимо настроить исключения для сертификата, указанного для скачивания потоков данных. В ходе фильтрации трафика SSL сертификат нельзя заменять.

Пропускная способность

Требования зависят от конкретного варианта использования и используемых потоков данных об угрозах. Дополнительные сведения о требованиях см. в руководстве по выбору аппаратной конфигурации.

Предоставление данных

«Лаборатория Касперского» как компания, занимающаяся кибербезопасностью, осуществляет обработку данных и статистики, имеющих отношение к киберугрозам. Эти данные включают в себя подозрительные и вредоносные файлы, а также статистику, позволяющую обнаруживать как известные киберугрозы, так и новое вредоносное ПО и новые методы атак. Под статистикой понимаются метаданные, т. е. дополнительная техническая информация о событиях, произошедших на устройстве пользователя, которую Kaspersky CyberTrace может отправлять в «Лабораторию Касперского» в зависимости от различных факторов, например, действия пользователя, параметры Kaspersky CyberTrace, конфигурация операционной системы, на которой установлен Kaspersky CyberTrace, и другое ПО, установленное в системе.

Подробная информация обо всех данных, обрабатываемых Kaspersky CyberTrace приведена в Лицензионном соглашении и Положении о Kaspersky Security Network (KSN).

О Kaspersky Security Network

Kaspersky Security Network (KSN) представляет собой сложную распределенную инфраструктуру, предназначенную для интеллектуальной обработки связанных с киберугрозами потоков индикаторов, добровольно предоставляемых миллионами пользователей по всему миру. Автоматический облачный анализ этих позволяет системе как можно быстрее реагировать на новые и ранее неизвестные угрозы. Это один из компонентов передового подхода «Лаборатории Касперского» к защите, сочетающего в себе экспертный анализ, алгоритмы машинного обучения и большие данные, что позволяет выявлять закономерности, изменения и новые киберугрозы.

Основные принципы работы Kaspersky Security Network:

- Обрабатывается только информация, необходимая для совершенствования алгоритмов обнаружения киберугроз, повышения точности работы продуктов и разработки новых улучшенных решений.
- Система получает информацию от пользователей, принявших Лицензионное соглашение и Положение о KSN, в котором подробно описаны типы получаемой информации.
- Положение о KSN можно принять или отклонить в любое время путем изменения параметров решения.
- Данные, принимаемые на стороне KSN, не привязаны к конкретным пользователям. Данные используются в форме агрегированной статистики на отдельных серверах со строгими политиками контроля доступа.
- Предоставляемые данные также защищаются во время передачи в соответствии с требованиями законодательства и самыми строгими отраслевыми стандартами: используются в том числе шифрование, цифровые сертификаты, сетевые экраны.

Предоставление данных путем их передачи из Kaspersky CyberTrace в KSN позволяет повысить скорость реагирования Kaspersky CyberTrace на угрозы информационной и сетевой безопасности за счет снижения вероятности ложных срабатываний и повышения эффективности работы компонентов Kaspersky CyberTrace.

Обработка персональных данных

Если обработка персональных данных является необходимым условием надлежащего функционирования решения или услуги, «Лаборатория Касперского» проводит анализ целей, объема и юридических оснований обработки персональных данных в соответствии с действующим законодательством. Состав обрабатываемых персональных данных всегда отвечает целям обработки. Решения и службы получают и обрабатывают данные в объеме, необходимом для надлежащего функционирования этих решений и служб.

В качестве персональных данных Kaspersky CyberTrace получает только идентификатор `source_id` потоков данных с целью идентификации потоков данных. После загрузки или обновления того или иного потока данных Kaspersky CyberTrace генерирует идентификатор `source_id` для загруженного или обновленного потока данных. Этот идентификатор хранится в базе данных с момента добавления потока данных в Kaspersky CyberTrace до момента удаления Kaspersky CyberTrace с устройства. В целях защиты данных Kaspersky CyberTrace обеспечивает обезличивание путей хранимых файлов.

Что нового

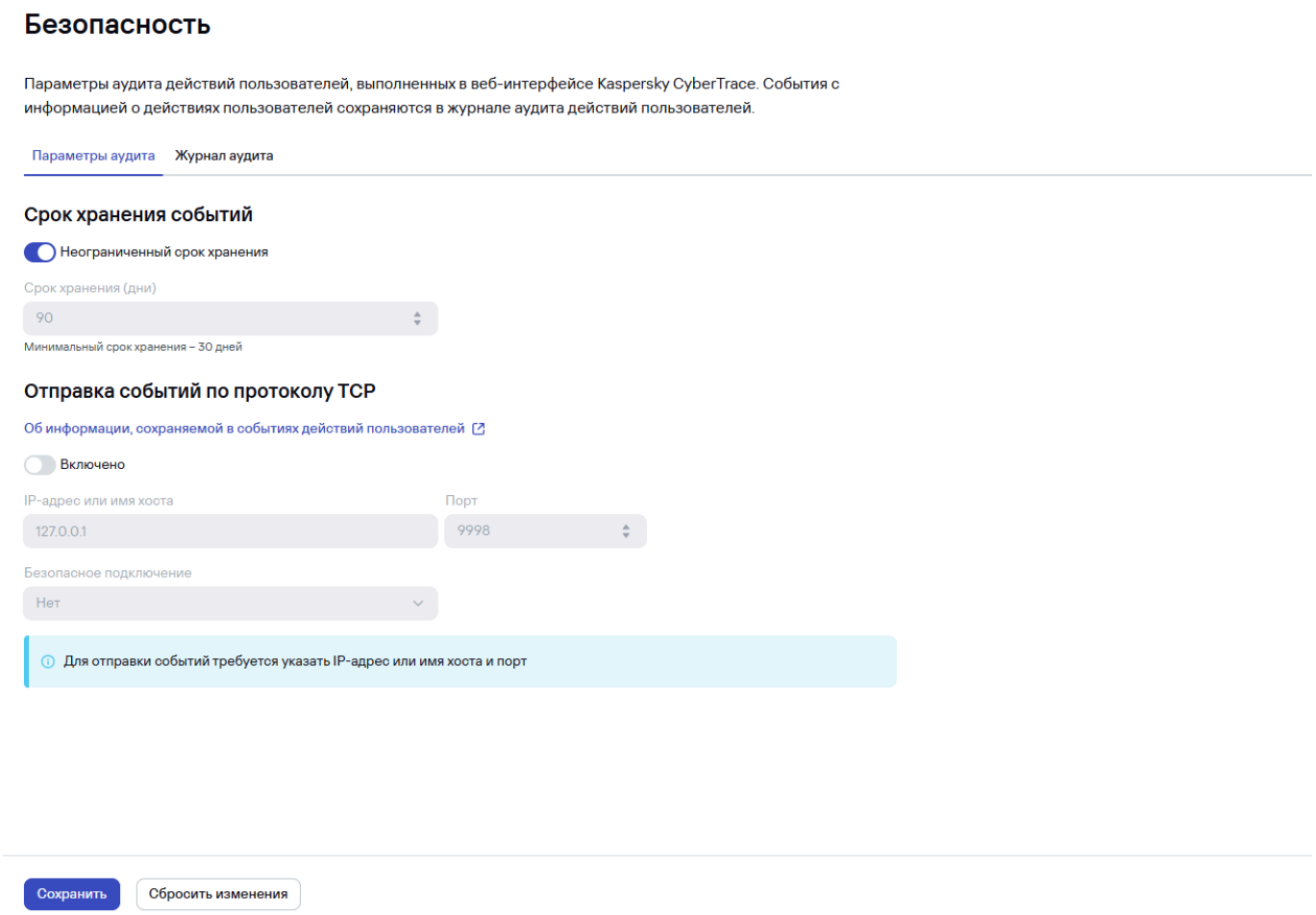
В Kaspersky CyberTrace были реализованы следующие новые возможности и улучшения:

Что нового в версии 5.4

- **Добавлен аудит безопасности и действий пользователей.**

  Информация о действиях пользователя в веб-интерфейсе Kaspersky CyberTrace, связанных с безопасностью, может автоматически сохраняться в виде событий в журнал аудита безопасности (см. рисунок ниже). Журнал аудита хранится локально на сервере, на котором установлен Kaspersky CyberTrace. При необходимости вы можете скачать файлы журнала аудита через веб-интерфейс Kaspersky CyberTrace. Вы также можете включить отправку событий по протоколу TCP в SIEM-систему для дальнейшего анализа.

  Если произойдет инцидент безопасности, связанный с Kaspersky CyberTrace, сотрудник службы безопасности сможет отследить, что именно произошло, изучив журнал аудита безопасности и действий пользователей. Эта функциональность также требуется для соответствия большинству норм и стандартов кибербезопасности, таким как ГОСТ, федеральные законы, приказы ФСТЭК и требования ФСБ.

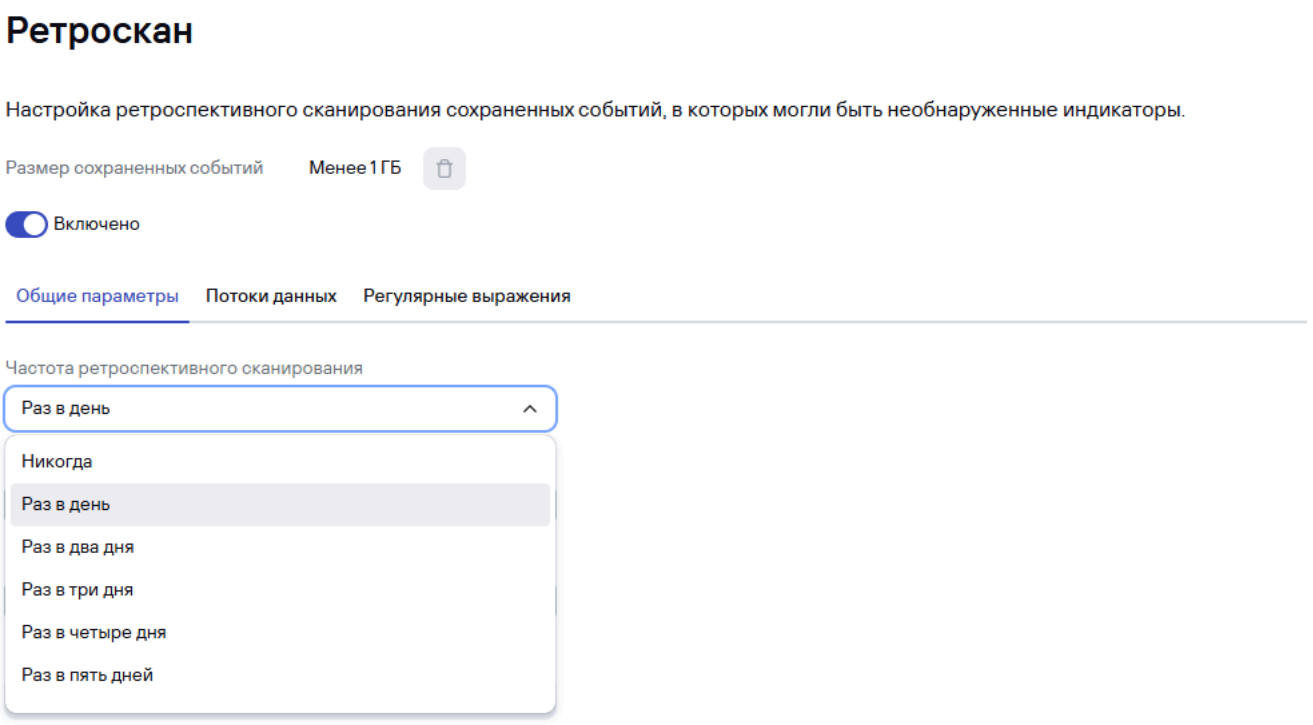


Параметры безопасности и аудита пользователей

- **Внесены значительные улучшения функциональности ретроспективного сканирования**:

  - Оптимизирована производительность ретроспективного сканирования, и его скорость по оценкам возросла в несколько раз (на основе измерений, полученных в тестовой инфраструктуре). Ретроспективное сканирование сохраненных событий безопасности теперь может запускаться чаще, что в свою очередь позволяет быстрее обнаруживать инциденты безопасности и значительно снижает среднее время обнаружения (MTTD).

  - Теперь вы можете установить периодичность ретроспективного сканирования на определенное количество дней (от одного до пяти) в дополнение к ранее доступным значениям (см. рисунок ниже). Это позволяет сканировать сохраненные события безопасности с необходимой периодичностью, которая зависит от размера сохраненных данных: новое сканирование на основе недавно полученных индикаторов компрометации может быть запущено сразу после того, как будут просканированы все имеющиеся данные, без необходимости ждать несколько дней. Это улучшение позволяет дополнительно снизить MTTD.

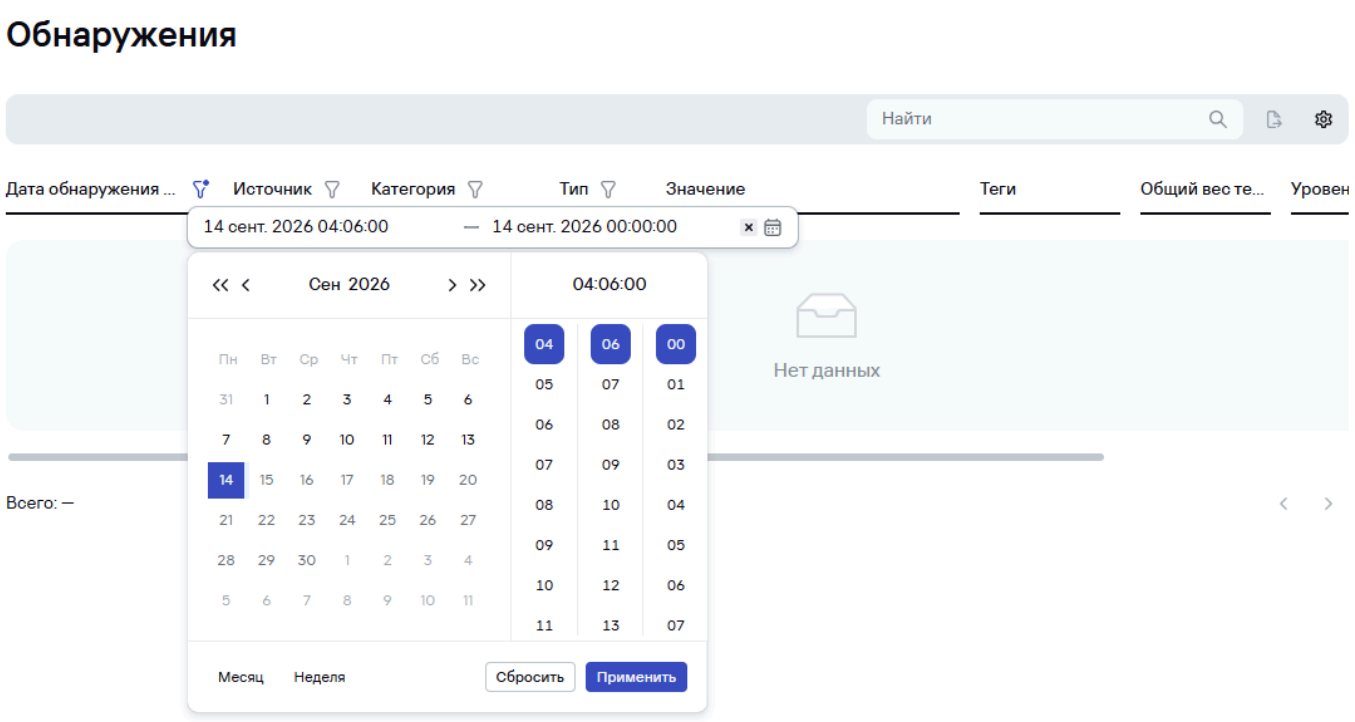


Возможные значения параметра **Частота ретроспективного сканирования**

  - Руководство по выбору аппаратной конфигурации обновлено и теперь содержит рекомендации по вычислительным ресурсам, необходимым для достижения определенной величины EPS с результатами сканирования в реальном времени, а также с включенным или выключенным ретроспективным сканированием. Рекомендации отличаются в зависимости от режима обработки данных (на основе TCP или API).

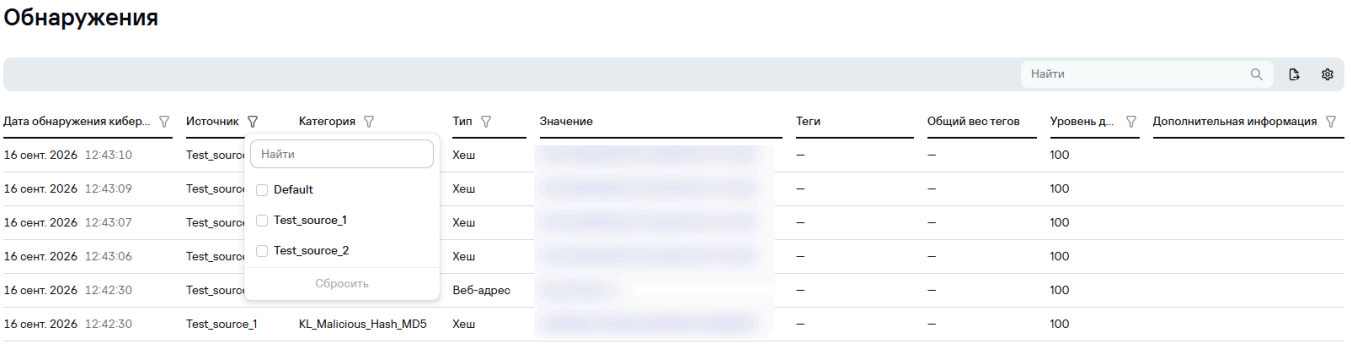
- **Улучшена фильтрация в таблице обнаружений**:

  - При фильтрации обнаружений по дате вы также можете указать пользовательский временной интервал (в часах и минутах). Если у вас большой поток событий безопасности и, следовательно, значительное количество событий обнаружений, вы можете применить этот фильтр, чтобы сосредоточиться на конкретном небольшом промежутке времени, в течение которого случился предполагаемый важный инцидент безопасности, без необходимости просматривать много страниц обнаружений с более низким приоритетом расследования. Это позволяет снизить MTTD.



Фильтрация обнаружений киберугроз по дате и времени с помощью столбца **Дата обнаружения киберугрозы**

  - Теперь вы можете фильтровать обнаружения по источнику, что позволяет сосредоточиться на важном источнике событий и снизить MTTR.



Фильтрация обнаружений киберугроз по источнику с помощью столбца **Источник**

- **Уровни лицензирования Community Edition и Matching Engine теперь предоставляют доступ к большему количеству функций:**

  - Уровень лицензирования Matching Engine теперь предоставляет доступ к API и многопользовательскому режиму. Эти функции позволяют обогащать события, полученные из SIEM-системы "Лаборатории Касперского" (Kaspersky Unified Monitoring and Analysis Platform), данными из Kaspersky Threat Intelligence Feeds, доступ к которым у вас уже может быть. Теперь вам не нужно приобретать полную коммерческую лицензию для доступа ко всем функциям Kaspersky CyberTrace (уровень лицензирования Enterprise TIP), чтобы использовать эту возможность.

  - Максимальное количество EPS на уровне лицензирования Community Edition теперь может быть увеличено с 250 до 500, если вы приняли положение, регламентирующее использование Kaspersky Security Network. Это предоставляет возможность опробовать Kaspersky CyberTrace в реальных сценариях в условиях производственной нагрузки. Помимо отдельных пользователей, средние предприятия с относительно небольшим количеством событий безопасности теперь также смогут начать работу с Kaspersky CyberTrace, чтобы оценить его эффективность.

- **Исправление ошибок**.

Руководства по установке и интеграции

В этой главе описывается порядок установки Kaspersky CyberTrace, настройки и интеграции с различными SIEM-системами.

Обзор установки и интеграции

В этом разделе описывается порядок установки и интеграции Kaspersky CyberTrace.

Введение

Kaspersky CyberTrace поддерживает интеграцию с множеством различных источников событий. Процедура установки и интеграции разделена на две части:

1. Установка Kaspersky CyberTrace

   Рекомендуется устанавливать Kaspersky CyberTrace с помощью одного из инсталляционных пакетов для используемой операционной системы. Для ОС Linux предоставляются пакеты DEB и RPM. Для ОС Windows предоставляется исполняемый файл установщика.

   После установки Kaspersky CyberTrace можно выполнить первоначальную настройку с помощью соответствующего мастера в веб-интерфейсе Kaspersky CyberTrace. В ходе этого процесса необходимо выбрать источник событий, например, SIEM-систему, задать для него параметры подключения и настроить обновления потоков данных об угрозах.

   > Если требуется использовать инкрементные версии Kaspersky Threat Data Feeds, необходимо включить их перед выполнением первоначальной настройки Kaspersky CyberTrace.

   После завершения первоначальной настройки Kaspersky CyberTrace по умолчанию использует параметры для заданного источника событий. Например, по умолчанию Kaspersky CyberTrace выполняет парсинг входящих событий с помощью регулярных выражений, заданных для выбранного источника событий, и использует формат специальный для сообщений об обнаруженных киберугрозах. При необходимости указанные параметры можно впоследствии изменить.

2. Интеграция Kaspersky CyberTrace с источником событий

   В этой части источник событий настраивается таким образом, чтобы он мог отправлять свои события в Kaspersky CyberTrace и получать сообщения об обнаруженных киберугрозах от Kaspersky CyberTrace. В зависимости от выбранного источника событий также можно установить определенные приложения и инструменты, работающие с событиями Kaspersky CyberTrace. Например, Kaspersky CyberTrace предоставляет приложения для Splunk® и QRadar, а также предварительно настроенную информационную панель для RSA NetWitness. Помимо приложений для определенных источников событий можно использовать утилиту LogScanner для отправки файлов журналов, IP-адресов, URL и хешей на проверку в Kaspersky CyberTrace.

Предварительные условия

Убедитесь, что сервер, предназначенный для работы Kaspersky CyberTrace, соответствует аппаратным и программным требованиям.

Убедитесь, что на сервере, на котором устанавливается Kaspersky CyberTrace, установлены точные значения даты и времени. Для получения точных значений даты и времени можно использовать NTP-сервер.

Для продуктов ArcSight перед установкой Kaspersky CyberTrace необходимо установить ArcSight SmartConnector. Для получения дополнительной информации см. разделы Предварительные условия (ArcSight) и Руководство по интеграции (ArcSight).

Часть 1. Установка Kaspersky CyberTrace

При установке Kaspersky CyberTrace устанавливаются и настраиваются все компоненты, необходимые для работы с потоками данных об угрозах, такие как Kaspersky CyberTrace Service и Feed Utility.

Kaspersky CyberTrace можно установить на любом хосте, который может получать события от выбранного источника событий, например, от SIEM-системы, межсетевого экрана или прокси-сервера. При настройке Kaspersky CyberTrace во время установки задается способ получения событий и отправки оповещений.

Kaspersky CyberTrace обязательно должен устанавливаться в соответствии с выбранной схемой интеграции. Например, если Kaspersky CyberTrace и SIEM-систему требуется установить на разные серверы, проверьте доступные схемы интеграции для данной SIEM-системы, чтобы определить, где следует установить Kaspersky CyberTrace.

Установите Kaspersky CyberTrace в порядке, описанном в разделе, соответствующем используемой операционной системе:

- Установка в ОС Linux
- Установка в ОС Windows

После установки Kaspersky CyberTrace выполните следующие действия:

- Если требуется использовать разные потоки данных об угрозах Kaspersky Threat Data Feeds, включите их.
- Если не требуется использовать инкрементные версии потоков данных об угрозах Kaspersky Threat Data Feeds, откройте веб-интерфейс Kaspersky CyberTrace и следуйте указаниям мастера первоначальной настройки.

Часть 2. Интеграция Kaspersky CyberTrace с источником событий

Для автоматического обнаружения IoC в журналах событий безопасности Kaspersky CyberTrace должен быть интегрирован с источником событий. Это может быть либо автономный источник событий (например, межсетевой экран или прокси-сервер), либо SIEM-система. Этот источник событий отправляет события в Kaspersky CyberTrace, а Kaspersky CyberTrace в свою очередь отправляет сообщения об обнаруженных угрозах в SIEM или другое приложение в соответствии с заданными настройками.

Поддерживаются следующие SIEM-системы:

- Kaspersky Unified Monitoring and Analysis Platform
- Splunk
- ArcSight
- QRadar
- RSA NetWitness
- LogRhythm
- McAfee Enterprise Security Manager
- AlienVault USM/OSSIM
- FortiSIEM
- Другие SIEM-систему и не-SIEM-системы

Руководство по выбору аппаратной конфигурации

В данном руководстве приведены рекомендации по вычислительным ресурсам (ЦП, ОЗУ и место на жестком диске) и пропускной способности сети, которые необходимы для установки и использования Kaspersky CyberTrace с обеспечением определенного уровня производительности.

Рекомендации зависят от режима обработки данных и планируемых к использованию функциональных возможностей (в частности, ретроспективного сканирования).

Рекомендуемые конфигурации в зависимости от режима

В этом разделе описываются минимальные аппаратные требования Kaspersky CyberTrace в зависимости от режима обработки данных и включенных функциональных возможностей. Для каждого режима также приводятся параметры Kaspersky CyberTrace, влияющие на производительность, которые были использованы при тестировании.

Kaspersky CyberTrace может обрабатывать поступающие данные в следующих режимах:

- Режим обработки событий на основе TCP.

  События передаются в Kaspersky CyberTrace по протоколу TCP в формате, используемом в той или иной SIEM-системе. Kaspersky CyberTrace выполняет парсинг этих событий с помощью регулярных выражений, адаптированных к соответствующему формату. Этот режим предъявляет повышенные требования к вычислительным ресурсам и обеспечивает более низкую производительность.

- Режим обработки индикаторов на основе API

  Индикаторы передаются в Kaspersky CyberTrace с помощью lookup-методов публичных API в определенном унифицированном формате. В этом режиме обеспечивается более высокая производительность.

Также возможна одновременная обработка событий с помощью TCP и индикаторов с помощью API, однако производительность при этом не гарантируется. Режим зависит от способа отправки данных источником событий, интегрированным с Kaspersky CyberTrace.

Кроме того, исключительно в целях оценки или демонстрации Kaspersky CyberTrace можно использовать в режиме оценки. В этом режиме Kaspersky CyberTrace работает с рядом ограничений, однако не требует больших вычислительных ресурсов.

О тестовом наборе

Расчетные значения, приведенные в этом разделе, получены на тестовом наборе со следующим распределением данных по типам индикаторов:

- IP-адреса составляют 33% тестового набора.
- Веб-адреса составляют 33% тестового набора.
- Хеши MD5 составляют 11% тестового набора.
- Хеши SHA1 составляют 11% тестового набора.
- Хеши SHA256 составляют 11% тестового набора.

Коэффициент обнаружения для этого тестового набора составляет 0,05%.

Рекомендации для режима оценки

Режим оценки обладает следующими характеристиками:

- Kaspersky CyberTrace активируется по лицензии Community Edition.
- Количество обрабатываемых событий в секунду (EPS) – 250.

  Значение EPS можно увеличить до 500, приняв Положение о Kaspersky Security Network.
- Используются только демонстрационные потоки данных.
- Ретроспективное сканирование включено.

- Срок хранения событий, используемых для ретроспективного сканирования, составляет один месяц.
- Срок хранения результатов ретроспективного сканирования составляет один месяц.

Минимальные требования для этого режима приведены в таблице ниже.

Требования к оборудованию для режима оценки

Операционная система	EPS	Логические процессоры	ОЗУ, ГБ	Место на диске, ГБ	Пропускная способность сети, Гбит/с
Windows или Linux	250	8	16	468: • 3 (для системных файлов, статистики и других служебных данных) • 0,93 (для сохраненных обнаружений) • 463,48 (для данных ретроспективного сканирования) • 0,37 (для индикаторов)	1

Рекомендации для режима обработки событий на основе TCP

Kaspersky CyberTrace должен быть активирован по коммерческой лицензии в режиме обработки событий по протоколу TCP. Мерой производительности служит максимальное количество событий в секунду (EPS), которое Kaspersky CyberTrace может обработать при данной конфигурации оборудования.

Тестирование Kaspersky CyberTrace в этом режиме выполнялось на тестовом наборе со следующими параметрами, которые могут влиять на EPS:

- **Коммерческие потоки данных включены.**
  - APT Hash Data Feed
  - APT IP Data Feed
  - APT URL Data Feed
  - Botnet C&C URL Data Feed
  - ICS Hash Data Feed
  - IP Reputation Data Feed
  - IoT URL Data Feed
  - Malicious Hash Data Feed
  - Malicious URL Data Feed
  - Mobile Botnet C&C URL Data Feed
  - Mobile Malicious Hash Data Feed
  - Phishing URL Data Feed
  - Ransomware URL Data Feed
- Количество индикаторов составляет 4,4 миллиона.

- Средняя длина события составляет 225 символов.
- Каждое событие содержит по 4 индикатора средней длиной 30 символов.

  В случае более длинных индикаторов фактическая производительность может снизиться.
- Коэффициент обнаружения составляет 0,05%.
- Потоки данных обновляются раз в час.
- Регулярное выражение для парсинга событий взято из шаблона для ArcSight или прочих SIEM-систем.
- Настроены 1 тенант и 1 источник.
- Запись в журнал отключена.
- Предоставление данных в Kaspersky Security Network отключено.
- Экспорт индикаторов отключен.
- Формирование отчетов отключено.
- Использование TLS для входящих событий отключено.

Рекомендуемая конфигурация и расчетное значение EPS различаются в зависимости от того, включено ли ретроспективное сканирование.

Режим обработки событий на основе TCP без ретроспективного сканирования

В этом режиме ретроспективное сканирование отключено.

Минимальные требования и расчетные значения EPS приведены в таблице ниже.

Требования к оборудованию без ретроспективного сканирования

Операционная система	Регулярные выражения	EPS	Логические процессоры	Объем оперативной памяти, ГБ	Место на диске в сутки, ГБ	Пропускная способность сети, Гбит/с
Windows или Linux	Другое	10 000	16	16	1,3	1
Windows или Linux	ArcSight	15 000	16	16	2	1
Windows или Linux	Другое	20 000	32	24	2,5	1
Windows или Linux	ArcSight	30 000	32	24	4	1
Windows или Linux	Другое	80 000	96	48	11	10
Windows или Linux	ArcSight	150 000	96	48	19	10

Режим обработки событий на основе TCP с ретроспективным сканированием

В этом режиме ретроспективное сканирование включено. Обратите внимание: если включено ретроспективное сканирование, необходимо выделить часть логических процессоров для обработки ретроспективных данных. Выделение логических процессоров для обработки входящих событий и данных ретроспективного сканирования также может влиять на EPS.

Минимальные требования и расчетные значения EPS приведены в таблице ниже.

Требования к оборудованию с ретроспективным сканированием

Операционная система	Регулярные выражения	EPS	Логические процессоры	Объем оперативной памяти, ГБ	Место на диске в сутки, ГБ	Пропускная способность сети, Гбит/с
Windows или Linux	Другое	6 000	16	16	147	1
Windows или Linux	ArcSight	12 000	16	16	373	1
Windows или Linux	Другое	15 000	32	32	378	1
Windows или Linux	ArcSight	28 000	32	32	905	1
Windows или Linux	Другое	70 000	96	48	1890	10
Windows или Linux	ArcSight	120 000	96	48	3726	10

Рекомендации для режима обработки индикаторов на основе API

Kaspersky CyberTrace должен быть активирован по коммерческой лицензии в режиме обработки индикаторов на основе API. Мерой производительности служит максимальное количество индикаторов в секунду (IPS), которое Kaspersky CyberTrace может обработать при данной конфигурации оборудования.

Тестирование Kaspersky CyberTrace в этом режиме выполнялось на тестовом наборе со следующими параметрами, которые могут влиять на IPS:

- **Коммерческие потоки данных включены.**
  - APT Hash Data Feed
  - APT IP Data Feed
  - APT URL Data Feed
  - Botnet C&C URL Data Feed
  - ICS Hash Data Feed
  - IP Reputation Data Feed
  - IoT URL Data Feed
  - Malicious Hash Data Feed
  - Malicious URL Data Feed
  - Mobile Botnet C&C URL Data Feed
  - Mobile Malicious Hash Data Feed
  - Phishing URL Data Feed
  - Ransomware URL Data Feed
- Количество индикаторов составляет 4,4 миллиона.

- Средняя длина индикатора составляет 30 символов.
- Коэффициент обнаружения составляет 0,05%.
- Потоки данных обновляются раз в час.
- Для парсинга событий используется регулярное выражение по умолчанию.
- Настроены 1 тенант и 1 источник.
- Запись в журнал отключена.
- Предоставление данных в Kaspersky Security Network отключено.
- Экспорт индикаторов отключен.
- Формирование отчетов отключено.

Рекомендуемая конфигурация и расчетное значение IPS различаются в зависимости от того, включено ли ретроспективное сканирование.

Режим обработки индикаторов на основе API без ретроспективного сканирования

В этом режиме ретроспективное сканирование отключено.

Минимальные требования и расчетные значения IPS приведены в таблице ниже.

Требования к оборудованию без ретроспективного сканирования

Операционная система	IPS	Логические процессоры	Объем оперативной памяти, ГБ	Место на диске в сутки, ГБ	Пропускная способность сети, Гбит/с
Windows или Linux	70 000	16	16	12	1
Windows или Linux	150 000	32	24	21	1
Windows или Linux	250 000	96	96	42	10

Режим обработки индикаторов на основе API с ретроспективным сканированием

В этом режиме ретроспективное сканирование включено. Обратите внимание: если включено ретроспективное сканирование, необходимо выделить часть логических процессоров для обработки ретроспективных данных. Выделение логических процессоров для обработки входящих событий и данных ретроспективного сканирования также может влиять на IPS.

Минимальные требования и расчетные значения IPS приведены в таблице ниже.

Требования к оборудованию с ретроспективным сканированием

Операционная система	IPS	Логические процессоры	Объем оперативной памяти, ГБ	Место на диске в сутки, ГБ	Пропускная способность сети, Гбит/с
Windows или Linux	30 000	16	16	470	1
Windows или Linux	70 000	32	32	1001	10
Windows или Linux	150 000	96	96	2100	10

Требования к процессору

Kaspersky CyberTrace поддерживает только архитектуру x86-64.

Рекомендуется устанавливать Kaspersky CyberTrace на высокопроизводительных серверах.

Важны два параметра процессора:

- количество ядер процессора;
- количество потоков процессора.

Например, процессор может обладать двумя ядрами и предоставлять четыре потока исполнения.

При выборе процессора обратите внимание на количество потоков исполнения, так как этот параметр больше влияет на производительность. В этом руководстве по масштабированию предполагается, что каждое ядро процессора обеспечивает два потока исполнения.

Для получения дополнительной информации о ядрах и потоках ЦП выполните поиск по запросу «Одновременная многопоточность» с помощью поисковой системы.

Исходя из количества ядер процессора, можно выбрать необходимое количество сканеров и потоков на каждый сканер для процесса Kaspersky CyberTrace Service.

В этом руководстве по масштабированию рекомендации по подбору конфигурации даются в «логических процессорах». Количество логических процессоров рассчитывается по формуле: <количество процессоров> × <количество ядер на процессор> × <количество потоков на ядро>

Сетевые требования

Приблизительный расчет пропускной способности сети выполняется по следующей формуле:

```
<пропускная способность (Гбит/с)> = <EPS> x <размер события в байтах> x 8 / (1000 x 1000 x1000)
```

Здесь:

- `<EPS>` – количество событий в секунду, обрабатываемых Kaspersky CyberTrace.
- `<размер события в байтах>` – приблизительный размер каждого события обнаружения киберугрозы в байтах. Может быть установлено значение до 2,5 КБ.

В соответствии с этой формулой и с учетом некоторого резерва пропускной способности рекомендуется использовать следующее правило:

- Если ваше запланированное EPS меньше 40 000, вам потребуется сеть со скоростью 1 Гбит/с.
- В противном случае вам потребуется сеть со скоростью 10 Гбит/с.

Требования к памяти

Чтобы использовать Kaspersky CyberTrace с базовым набором потоков данных «Лаборатории Касперского», требуется как минимум 16 ГБ оперативной памяти.

> Указанный выше объем памяти должен быть доступен для Kaspersky CyberTrace. При выборе общего объема оперативной памяти учитывайте потребление памяти операционной системой и другими приложениями.

В базовый набор потоков данных входят следующие потоки данных:

- APT Hash Data Feed
- APT IP Data Feed
- APT URL Data Feed
- Botnet C&C URL Data Feed
- ICS Hash Data Feed
- IoT URL Data Feed
- IP Reputation Data Feed
- Malicious Hash Data Feed
- Malicious URL Data Feed
- Mobile Botnet C&C URL Data Feed
- Mobile Malicious Hash Data Feed
- Phishing URL Data Feed
- Ransomware URL Data Feed

Требования к диску

Тип диска

Тип диска зависит от количества событий в секунду (EPS), обрабатываемых Kaspersky CyberTrace:

- Если EPS не превышает 10 000, можно использовать жесткий диск (HDD).
- Если EPS больше 10 000, рекомендуется использовать твердотельный накопитель (SSD).

Свободное место на диске

Объем свободного места на диске рассчитывается отдельно для следующих данных:

- Системные файлы, статистика и другие служебные данные.
- Сохраненные обнаружения.
- Данные ретроспективного сканирования.
- Индикаторы.

После этого полученные значения суммируются, чтобы получить итоговое значение.

Место на диске для системных файлов, статистики и других служебных данных

На каждый месяц хранения статистики требуется около 1 ГБ свободного места на диске (статистика хранится до трех месяцев).

Место на диске для сохраненных обнаружений

Размер сохраненных обнаружений киберугроз и данных ретроспективного сканирования зависит от регулярных выражений, используемых для парсинга событий.

В случае регулярных выражений по умолчанию объем дискового пространства рассчитывается следующим образом:

```
<дисковое пространство> = <EPS> x <уровень обнаружения> x <размер обнаружения> x 3600 x 24 x <период хранения статистики>
```

Параметры здесь имеют следующий смысл:

- `<EPS>` – количество событий в секунду, обрабатываемых Kaspersky CyberTrace.
- `<уровень обнаружения>` – приблизительный процент обнаружений относительно EPS. Может быть установлено значение 0,05% или 0,0005.
- `<размер обнаружения>` – приблизительный размер данных каждого события обнаружения. Может быть установлено значение до 2,5 КБ.
- `<период хранения статистики>` – период в днях, в течение которого сохраняются события, использованные для ретроспективного сканирования.

Место на диске для данных ретроспективного сканирования

Размер сохраненных данных ретроспективного сканирования зависит от регулярных выражений, используемых для парсинга событий, и от состава данных, отмеченных для сохранения.

В случае регулярных выражений по умолчанию объем дискового пространства рассчитывается следующим образом:

```
<дисковое пространство> = <EPS> x <размер события> x 3600 x 24 x <срок хранения для ретроспективного сканирования>
```

Параметры здесь имеют следующий смысл:

- `<EPS>` – количество событий в секунду, обрабатываемых Kaspersky CyberTrace.
- `<размер события>` – приблизительный размер данных одного сохраняемого события. Может быть установлено значение до 0,25 КБ.
- `<срок хранения для ретроспективного сканирования>` – период в днях, в течение которого сохраняются результаты ретроспективного сканирования.

Место на диске для индикаторов

Это значение выбирается следующим образом:

- Если вы используете демонстрационные потоки данных об угрозах, это значение составляет 0,37 ГБ.
- Если вы используете типичный набор коммерческих потоков данных об угрозах, это значение составляет 6 ГБ.
- При добавлении или удалении используемых потоков данных это значение соответствующим образом увеличивается или уменьшается.

Рекомендации по настройке Kaspersky CyberTrace

В этой статье приведены рекомендации по расчету значений параметров Kaspersky CyberTrace, связанных с обработкой данных, обеспечивающих повышение производительности Kaspersky CyberTrace. В зависимости от режима обработки (TCP или API) Kaspersky CyberTrace обрабатывает поступающие данные следующим образом:

- В режиме обработки событий на основе TCP каждое входящее TCP-соединение обрабатывается как *отдельная* очередь. Для каждой очереди выделяется определенное количество потоков исполнения.
- В режиме обработки индикаторов на основе API все входящие API-запросы обрабатываются в *единой* очереди. Для обработки этой очереди и извлечения индикаторов выделяется определенное количество потоков исполнения.

Рекомендации для режима обработки событий на основе TCP

Для режима обработки событий на основе TCP в конфигурационном файле необходимо настроить следующие параметры, влияющие на EPS:

- `ScannersCount` – максимальное количество сканеров, осуществляющих обработку, равное или большее по отношению к количеству входящих TCP-соединений.
- `ScanningThreadsPerScanner` – максимальное количество потоков исполнения для каждого сканера.

Рекомендуется также оставить не менее двух ядер (или не менее четырех логических процессоров) свободными для выполнения фоновых задач.

Если ретроспективное сканирование *отключено*, количество сканеров и потоков исполнения на сканер должно удовлетворять следующим двум условиям:

- Значение `ScanningThreadsPerScanner` должно быть меньше, чем `< количество логических процессоров > / ScannersCount`.
- Значение `ScannersCount × ScanningThreadsPerScanner + ScannersCount` должно быть меньше, чем `< количество логических процессоров >`.

Если ретроспективное сканирование *включено*, необходимо также выделить часть потоков исполнения для считывания и анализа данных ретроспективного сканирования. В этом случае количество сканеров и потоков на сканер должно удовлетворять следующему условию:

```
< количество логических процессоров > = ScannersCount × ScanningThreadsPerScanner +
ScannersCount + retroscan_task_threads_for_reading +
retroscan_task_threads_for_analysis + < количество свободных логических процессоров >
```

Рекомендации для режима обработки индикаторов на основе API

Для режима обработки индикаторов на основе API в конфигурационном файле необходимо настроить следующие параметры, влияющие на IPS:

- `InFlightRequestLimit` – максимальное количество одновременно обрабатываемых API-запросов с данными индикаторов (при превышении этого количества возникает ошибка).

  > Этот параметр не влияет на IPS, но влияет на время отклика: чем меньше запросов, тем быстрее отклик.

- `WorkerThreadsCount` – общее количество потоков исполнения для обработки всех API-индикаторов.
- `DispatcherThreadsCount` – общее количество потоков исполнения, извлекающих индикаторы из событий и отправляющих их в очередь на обработку.

  По умолчанию количество потоков диспетчера равно 1. Для высоконагруженных систем с 16 или 32 процессорными ядрами рекомендуется установить значение 2 или более.

Рекомендуется также оставить не менее двух ядер (или не менее четырех логических процессоров) свободными для выполнения фоновых задач.

Если ретроспективное сканирование *отключено*, количество потоков исполнения должно удовлетворять следующим двум условиям:

- Значение `WorkerThreadsCount + DispatcherThreadsCount` должно быть меньше, чем `< количество логических процессоров >`.
- `WorkerThreadsCount = < количество логических процессоров > - DispatcherThreadsCount - < количество свободных логических процессоров >`.

Если ретроспективное сканирование *включено*, необходимо также выделить часть потоков исполнения для считывания и анализа данных ретроспективного сканирования: `retroscan_task_threads_for_reading` и `retroscan_task_threads_for_analysis`. В этом случае количество потоков исполнения должно удовлетворять следующему условию:

<количество логических процессоров> = WorkerThreadsCount + DispatcherThreadsCount + retroscan_task_threads_for_reading + retroscan_task_threads_for_analysis + <количество свободных логических процессоров>

Примеры расчетов

В таблице ниже приведены примеры расчета значений параметров в зависимости от режима обработки Kaspersky CyberTrace и количества логических процессоров. В каждом расчете для фоновых задач выделяется не менее четырех логических процессоров.

Примеры расчетов

Логические процессоры	Режим	ScannersCount	ScanningThreadsPerScanner	InFlightRequestLimit	WorkerThreadsCount	Dispatche
16	TCP без ретроспективного сканирования	2	6	Не применимо	Не применимо	Не приме
16	TCP с ретроспективным сканированием	2	4	Не применимо	Не применимо	Не приме
16	API без ретроспективного сканирования	Не применимо	Не применимо	50	10	2
16	API с ретроспективным сканированием	Не применимо	Не применимо	50	5	2
32	TCP без ретроспективного сканирования	4	7	Не применимо	Не применимо	Не приме
32	TCP с ретроспективным сканированием	4	5	Не применимо	Не применимо	Не приме
32	API без ретроспективного сканирования	Не применимо	Не применимо	100	26	2
32	API с ретроспективным сканированием	Не применимо	Не применимо	100	16	2
96	TCP без ретроспективного сканирования	4	23	Не применимо	Не применимо	Не приме
96	TCP с ретроспективным сканированием	4	15	Не применимо	Не применимо	Не приме
96	API без ретроспективного сканирования	Не применимо	Не применимо	100	88	4
96	API с ретроспективным сканированием	Не применимо	Не применимо	100	54	3
96	Гибрид API и TCP без ретроспективного сканирования	4	15	100	28	4
96	Гибрид API и TCP с ретроспективным сканированием	4	15	100	10	3

Часть 1. Установка Kaspersky CyberTrace

В этих разделах описывается порядок установки Kaspersky CyberTrace в ОС Linux и Windows.

Установка в ОС Linux

В этом разделе описывается порядок установки Kaspersky CyberTrace в ОС Linux.

Рекомендуется перед установкой Kaspersky CyberTrace установить и запустить антивирусное программное обеспечение.

В результате установки Kaspersky CyberTrace в операционной системе создаются две службы:

- `cybertrace_db` (служба, связанная с работой базы данных индикаторов)
- `cybertrace` (основная служба продукта)

Способы установки

В ОС Linux Kaspersky CyberTrace можно установить двумя способами:

- Установка пакета RPM

  При этом типе установки запускается скрипт установки `run.sh`. Скрипт установки устанавливает пакет RPM и запускает конфигуратор. Конфигуратор генерирует сертификаты для веб-интерфейса Kaspersky CyberTrace и настраивает базу данных индикаторов Elasticsearch.

  По умолчанию Elasticsearch создает свой временный каталог в `/tmp`. Однако в некоторых случаях в Linux `/tmp` по умолчанию монтируется с параметром `noexec`. Это может привести к некорректной работе базы данных индикаторов Elasticsearch. Чтобы этого избежать, `/tmp` следует монтировать с параметром `exec`.

- Установка пакета DEB

  Аналогична установке пакета RPM.

Установка пакета RPM

Kaspersky CyberTrace устанавливается в каталог `/opt/kaspersky/ktfs`. В этом документе этот каталог будет именоваться `%service_dir%`.

Учетная запись пользователя, выполняющего установку пакета RPM, должна иметь права root.

Чтобы установить пакет RPM Kaspersky CyberTrace, выполните следующие действия:

1. Распакуйте содержимое комплекта поставки в любой каталог на сервере. В следующей команде замените `%temp_dir%` на этот каталог и `%VERSION%` на версию инсталляционного пакета.

   ```
   tar -C %temp_dir% -xvzf Kaspersky_CyberTrace-Linux-x86_64-%VERSION%-RPM.tar.gz --no-same-owner
   ```

   Пакет RPM, скрипт установки и документация распаковываются в этот каталог.

   У архива может быть другое имя, например `%SIEM%-rpm.tar.gz`. Можно использовать имя как есть или переименовать архив командой `mv`.

2. Запустите скрипт установки:

   ```
   ./run.sh install
   ```

   Скрипт установки установит пакет RPM и добавит Kaspersky CyberTrace Service в список служб с помощью `chkconfig`. Kaspersky CyberTrace Service будет запускаться автоматически при загрузке системы.

   После установки пакета RPM скрипт установки автоматически запускает конфигуратор.

3. Выполните первоначальную настройку с помощью мастера первоначальной настройки.

Установка пакета DEB

Kaspersky CyberTrace устанавливается в каталог `/opt/kaspersky/ktfs`. В этом документе этот каталог будет именоваться `%service_dir%`.

Учетная запись пользователя, выполняющего установку пакета DEB, должна иметь права root.

Чтобы установить пакет DEB Kaspersky CyberTrace, выполните следующие действия:

1. Распакуйте содержимое комплекта поставки в любой каталог на сервере. В следующей команде замените `%temp_dir%` на этот каталог и `%VERSION%` на версию инсталляционного пакета.

   ```
   tar -C %temp_dir% -xvzf Kaspersky_CyberTrace-Linux-x86_64-%VERSION%-DEB.tar.gz --no-same-owner
   ```

   Пакет DEB, скрипт установки и документация распаковываются в этот каталог.

   У архива может быть другое имя, например `%SIEM%-deb.tar.gz`. Можно использовать имя как есть или переименовать архив командой `mv`.

2. Запустите скрипт установки:

```
./run.sh install
```

Скрипт установки установит пакет DEB и добавит Kaspersky CyberTrace Service в список служб, которые `systemd` запускает при загрузке системы. Kaspersky CyberTrace Service будет запускаться автоматически при загрузке системы.

3. После установки пакета DEB скрипт установки автоматически запускает конфигуратор.

4. Выполните первоначальную настройку с помощью мастера первоначальной настройки.

Интерактивная настройка с помощью конфигуратора

Чтобы выполнить интерактивную настройку с помощью конфигуратора, выполните следующие действия:

1. В конфигураторе примите Лицензионное соглашение (EULA):

   Используйте клавиши **PAGE UP** и **PAGE DOWN** для перехода. Чтобы выйти, введите **q**.

   Чтобы принять Лицензионное соглашение (EULA), введите `Yes`.

2. Если конфигуратор не определяет автоматически порты для веб-интерфейса Kaspersky CyberTrace и базы данных Elastic, укажите эту информацию.

3. После этого будет запущен Kaspersky CyberTrace. Будут отображены две ссылки:

   - Ссылка на веб-интерфейс Kaspersky CyberTrace.
   - Ссылка на документацию Kaspersky CyberTrace, где приведены учетные данные для входа в веб-интерфейс Kaspersky CyberTrace.

После установки

Убедитесь, что к каталогу, в котором установлен Kaspersky CyberTrace, имеют доступ только пользователи с правами root.

Если устройство, на котором установлен Kaspersky CyberTrace, защищено приложением Kaspersky Endpoint Security, рекомендуется настроить его.

Установка в ОС Windows

В этом разделе описывается порядок установки Kaspersky CyberTrace в ОС Windows.

> Рекомендуется перед установкой Kaspersky CyberTrace установить и запустить антивирусное программное обеспечение.

В результате установки Kaspersky CyberTrace в операционной системе создаются две службы:

- `cybertrace-elasticsearch` (служба, связанная с работой базы данных индикаторов)
- `cybertrace` (основная служба продукта)

Способы установки

В операционных системах Windows вы можете установить Kaspersky CyberTrace, запустив исполняемый файл установщика. В ходе установки установщик генерирует сертификаты для веб-интерфейса Kaspersky CyberTrace и настраивает базу данных индикаторов Elasticsearch.

Чтобы установить Kaspersky CyberTrace с помощью исполняемого файла установщика:

1. Убедитесь, что сервер, предназначенный для работы Kaspersky CyberTrace Service, соответствует аппаратным и программным требованиям.
2. Убедитесь, что сервер может отправлять оповещения на компьютер, на котором установлена SIEM-система, и может получать события от компьютера SIEM.
3. Запустите исполняемый файл установщика с расширением .exe.

   > Исполняемый файл установщика необходимо запускать под учетной записью администратора.

   При запуске файла .exe можно указать необязательный параметр `/accepteula`. Если указан этот параметр, установщик выполняет установку, не запрашивая каких-либо действий пользователя. Этот параметр можно указать, только если вы прочитали и приняли Лицензионное соглашение (EULA). Документ с текстом Лицензионного соглашения (EULA) входит в комплект поставки. Указывать этот параметр при установке Kaspersky CyberTrace не рекомендуется.
4. Примите Лицензионное соглашение (EULA).

   > Если установка будет продолжена, Kaspersky CyberTrace будет установлен в папку `C:\Program Files\Kaspersky Lab\Kaspersky CyberTrace`. В этом документе эта папка будет именоваться `%service_dir%`.
5. Запускается веб-интерфейс Kaspersky CyberTrace. Отобразится флажок и ссылка на веб-интерфейс Kaspersky CyberTrace:
   - По умолчанию после установки выполняется перенаправление на страницу веб-интерфейса Kaspersky CyberTrace. Уберите этот флажок, если не хотите переходить в веб-интерфейс пользователя.
   - Перейдите по ссылке документации Kaspersky CyberTrace, чтобы получить учетные данные для входа в веб-интерфейс Kaspersky CyberTrace.

Чтобы настроить Kaspersky CyberTrace после установки:

1. Выполните первоначальную настройку с помощью мастера первоначальной настройки.
2. Убедитесь в работоспособности всех установленных элементов. См. подраздел «Проверка работы компонентов Kaspersky CyberTrace» ниже.

Проверка работы компонентов Kaspersky CyberTrace

Убедитесь, что служба запущена, с помощью Диспетчера управления службами (SCM) и следующей команды:

```
sc query cybertrace
```

Подробные сведения приведены в разделе Управление Kaspersky CyberTrace Service с помощью SCM (Windows).

После установки

Убедитесь, что к папке, в которую установлен Kaspersky CyberTrace, имеют доступ только пользователи с правами root.

Если устройство, на котором установлен Kaspersky CyberTrace, защищено приложением Kaspersky Endpoint Security, рекомендуется настроить его.

Первоначальная настройка (мастер первоначальной настройки)

В этом разделе объясняется порядок настройки Kaspersky CyberTrace с помощью мастера первоначальной настройки.

Мастер первоначальной настройки — это последовательность страниц веб-интерфейса, на которых выполняется настройка Kaspersky CyberTrace после установки. После завершения работы мастера становятся доступными другие страницы веб-интерфейса.

Чтобы перейти к мастеру первоначальной настройки, выполните следующие действия:

1. Откройте веб-интерфейс Kaspersky CyberTrace в своем браузере по адресу `https://127.0.0.1`.
2. Войдите в веб-интерфейс Kaspersky CyberTrace с предустановленной учетной записью.

Пройдите следующие шаги мастера, нажимая на кнопку **Далее**.

Шаг 1. Страница приветствия

На шаге мастера **Добро пожаловать в Kaspersky CyberTrace** отображается краткая информация о Kaspersky CyberTrace и о мастере первоначальной настройки.

Шаг 2. Положение о Kaspersky Security Network (KSN)

На шаге **Положение о Kaspersky Security Network** вы можете принять или отклонить положение, регламентирующее использование KSN.

Чтобы выбрать статус Положения о KSN, выполните следующие действия:

1. Прочтите Положение о KSN, прокрутив поле с текстом документа до самого конца.
2. Выберите один из следующих вариантов:
   - **Я принимаю Положение о KSN**
   - **Я не принимаю Положение о KSN**
3. Нажмите на кнопку **Далее**.

   Статус Положения о KSN будет выбран.

Вы также можете выбрать статус Положения о KSN в разделе **Параметры** → **Служба** веб-интерфейса Kaspersky CyberTrace в режиме **Управление системой**.

Информацию о Kaspersky Security Network см. в статье Предоставление данных.

Шаг 3. Настройка прокси-сервера

На шаге мастера **Настройка прокси-сервера** можно задать параметры прокси-сервера. Этот шаг не является обязательным. Эти же настройки хранятся в конфигурационных файлах kl_feed_util.conf и kl_feed_service_log.conf.

Чтобы задать параметры прокси-сервера, выполните следующие действия:

1. Включите переключатель **Работать через прокси-сервер**.
2. В поле **IP-адрес или имя хоста** укажите IP-адрес или имя хоста прокси-сервера.

   Эта настройка хранится в элементе `Host` файла kl_feed_util.conf.
3. В поле **Порт** укажите порт прокси-сервера.

   Эта настройка хранится в элементе `Port` файла kl_feed_util.conf.

4. Если для доступа к прокси-серверу требуются учетные данные, выполните следующие действия:

   a. Включите переключатель **Использовать учетные данные для подключения к прокси-серверу**.

   b. В поле **Имя пользователя** укажите имя пользователя для доступа к прокси-серверу.

      Эта настройка хранится в зашифрованном виде в элементе `User` файла kl_feed_util.conf.

   c. В поле **Пароль** укажите пароль для доступа к прокси-серверу.

      Эта настройка хранится в зашифрованном виде в элементе `Password` файла kl_feed_util.conf.

> Для прокси-сервера можно использовать адрес IPv6.

В дальнейшем изменить настройки прокси-сервера можно будет на странице **Параметры → Служба** веб-интерфейса Kaspersky CyberTrace.

Шаг 4. Настройка лицензирования

На шаге мастера **Настройка лицензирования** можно добавить лицензионный ключ для активации Kaspersky CyberTrace.

Чтобы указать лицензию для активации Kaspersky CyberTrace, необходимо выполнить следующие действия:

1. Выберите требуемый уровень лицензирования Kaspersky CyberTrace: Community Edition или коммерческую лицензию.

   Community Edition предназначается для использования в ознакомительных целях с рядом ограничений.

   При выборе варианта **Community Edition** каких-либо дополнительных действий не потребуется.

2. Если же выбран коммерческий уровень лицензирования, необходимо выбрать метод добавления лицензионного ключа: с помощью кода активации или с помощью файла лицензионного ключа.

3. В зависимости от выбранного метода выполните следующие действия:

   - Введите код активации, полученный от вашего менеджера по работе с клиентами.

     Код активации состоит из четырех блоков по пять символов.

   - Нажмите кнопку **Выбрать**, затем выберите файл лицензионного ключа, полученный от вашего менеджера по работе с клиентами.

В дальнейшем управлять лицензионными ключами можно будет на странице **Параметры → Лицензирование** веб-интерфейса Kaspersky CyberTrace.

Шаг 5. Настройка службы

На шаге мастера **Настройка службы** можно задать пороговый EPS системы, настроить отправку служебных оповещений, а также указать IP-адрес или имя хоста сервера, на котором установлен Kaspersky CyberTrace. Эти же настройки хранятся в конфигурационных файлах kl_feed_util.conf и kl_feed_service_log.conf.

Чтобы задать настройки службы, выполните следующие действия:

1. В разделе **Пороговый EPS системы** настройте пороговый EPS системы (общее число событий в секунду — events per second):

   a. Включите переключатель.

   b. В поле **Пороговый EPS** введите требуемое значение порогового EPS.

   > Если пороговый EPS системы определяется лицензией, в веб-интерфейсе Kaspersky CyberTrace его изменить невозможно.

   > Если не задать пороговый EPS системы, можно столкнуться с непредвиденной деградацией производительности системы.

2. В разделе **Служебные оповещения** настройте отправку служебных оповещений, посредством которых другое ПО (например, SIEM-система) снабжается информацией о состоянии Kaspersky CyberTrace Service. Для этого выполните действия в следующем порядке:

   a. Включите переключатель.

   b. В полях **IP-адрес** и **Порт** укажите параметры сервера, на который требуется отправлять служебные оповещения.

   По умолчанию указаны IP-адрес `127.0.0.1` и порт `9999`.

   > Поддерживается отправка служебных оповещений на адреса IPv6.

   Эти настройки хранятся в элементе `OutputSettings > AlertConnectionString` файла kl_feed_service.conf.

3. В разделе **Веб-интерфейс** укажите IP-адрес или имя хоста, используемые для подключения к веб-интерфейсу Kaspersky CyberTrace. Это IP-адрес или имя хоста того сервера, на котором установлен Kaspersky CyberTrace и который используется, например, для скачивания отчетов об экспорте индикаторов.

   > В качестве адреса веб-интерфейса можно использовать адрес IPv6.

   Эта настройка хранится в элементе `ResourcesIP` файла kl_feed_service.conf.

   По умолчанию указан адрес `127.0.0.1`.

В дальнейшем изменить настройки службы можно будет на странице **Параметры → Служба** веб-интерфейса Kaspersky CyberTrace.

Шаг 6. Настройка управления данными

На шаге мастера **Настройка управления данными** необходимо выбрать и настроить SIEM-систему для интеграции с Kaspersky CyberTrace. Эти же настройки хранятся в конфигурационных файлах kl_feed_util.conf и kl_feed_service_log.conf.

От выбора SIEM-системы зависит формат конфигурационных файлов Kaspersky CyberTrace, поскольку эти файлы адаптируются под конкретную SIEM-систему.

Поддерживаются следующие SIEM-системы:

- Kaspersky Unified Monitoring and Analysis Platform
- Splunk
- ArcSight
- QRadar
- RSA NetWitness
- LogRhythm

Чтобы задать параметры управления данными, выполните следующие действия:

1. В разделе **SIEM-система** выберите SIEM-систему, с которой требуется интегрировать Kaspersky CyberTrace.
2. В разделе **Входящие события** задайте параметры сокета, который Kaspersky CyberTrace должен прослушивать в ожидании входящих событий:

   a. Выберите тип соединения, который требуется использовать: **IP-адрес и порт** или **Сокет UNIX**.

   b. В зависимости от типа подключения выполните одно из следующих действий:

   - Укажите IP-адрес и порт в полях **IP-адрес** и **Порт**.
   - В поле **Сокет UNIX** укажите сокет UNIX.

   Эти настройки хранятся в элементе `InputSettings > ConnectionString` файла kl_feed_service.conf.
3. В разделе **Оповещения об обнаружении индикаторов компрометации** укажите IP-адрес и порт, которые будут использоваться в Kaspersky CyberTrace для отправки оповещений об обнаружении индикаторов компрометации.

   Эти настройки хранятся в элементе `OutputSettings > ConnectionString` файла kl_feed_service.conf.

Для приема входящих событий и отправки исходящих оповещений можно использовать IPv6-адреса.

В дальнейшем изменить настройки службы можно будет на странице **Параметры → Общие** веб-интерфейса Kaspersky CyberTrace.

Шаг 7. Настройка сертификата

На шаге мастера **Настройка сертификата** можно добавить сертификат. Сертификат определяет набор потоков данных «Лаборатории Касперского» об угрозах, которые можно использовать в Kaspersky CyberTrace.

Чтобы указать сертификат, который требуется добавить в Kaspersky CyberTrace, выполните следующие действия:

1. Выберите необходимый тип сертификата: **Демо-сертификат** или **Коммерческий сертификат**.

   Демо-сертификат входит в комплект поставки и позволяет работать с демонстрационными версиями потоков данных «Лаборатории Касперского» об угрозах.

   При выборе варианта **Демо-сертификат** каких-либо дополнительных действий не потребуется.

2. При выборе варианта **Коммерческий сертификат** необходимо нажать на кнопку **Выбрать** и указать путь к файлу .pem с сертификатом.

В дальнейшем управлять сертификатами можно будет на странице **Параметры → Потоки данных** веб-интерфейса Kaspersky CyberTrace.

Шаг 8. Настройка потоков данных

На шаге мастера **Настройка потоков данных** укажите потоки данных, которые планируется использовать в Kaspersky CyberTrace.

Набор доступных потоков данных определяется сертификатом, выбранным на предыдущем шаге мастера.

Чтобы указать потоки данных, которые требуется использовать в Kaspersky CyberTrace, выполните следующие действия:

Установите флажки рядом с потоками данных, которые требуется использовать, и снимите флажки рядом с потоками данных, которые использовать не требуется.

В дальнейшем управлять потоками данных можно будет на странице **Параметры → Потоки данных** веб-интерфейса Kaspersky CyberTrace.

Шаг 9. Первоначальная настройка завершена

По завершении первоначальной настройки предлагается обратиться к документации Kaspersky CyberTrace. Отображаемые ссылки предназначены для следующих действий:

- Интеграция Kaspersky CyberTrace с используемой SIEM-системой
- Настройка дополнительных тенантов
- Ознакомьтесь с разделом Руководства администратора

Чтобы завершить работу мастера первоначальной настройки, нажмите кнопку **Готово**.

Настройка Kaspersky Endpoint Security

Если устройство, на котором установлен Kaspersky CyberTrace, защищено приложением Kaspersky Endpoint Security, рекомендуется настроить его в соответствии с описанием в этом разделе. В противном случае не исключено неожиданное снижение производительности системы.

Настройка Kaspersky Endpoint Security для Windows

Чтобы настроить Kaspersky Endpoint Security для Windows, выполните следующие действия:

1. Добавьте следующие пути в список исключений из проверки:
   - %ProgramFiles%\Kaspersky Lab\Kaspersky CyberTrace\feeds
   - %ProgramFiles%\Kaspersky Lab\Kaspersky CyberTrace\httpsrv\etc
   - %ProgramFiles%\Kaspersky Lab\Kaspersky CyberTrace\ioc_exports
   - %ProgramFiles%\Kaspersky Lab\Kaspersky CyberTrace\modules\elasticsearch\data
   - %ProgramFiles%\Kaspersky Lab\Kaspersky CyberTrace\var
2. Добавьте следующие процессы в список доверенных приложений:
   - %ProgramFiles%\Kaspersky Lab\Kaspersky CyberTrace\bin\kl_feed_service.exe
   - %ProgramFiles%\Kaspersky Lab\Kaspersky CyberTrace\bin\kl_balancer.exe
   - %ProgramFiles%\Kaspersky Lab\Kaspersky CyberTrace\modules\elasticsearch\bin\elasticsearch-service-x64.exe
   - %ProgramFiles%\Kaspersky Lab\Kaspersky CyberTrace\plugins\virus_total\virus_total.exe
   - %ProgramFiles%\Kaspersky Lab\Kaspersky CyberTrace\tools\kl_feed_compiler.exe

Более подробные сведения о настройке Kaspersky Endpoint Security для Windows приведены в справке Kaspersky Endpoint Security для Windows.

Настройка Kaspersky Endpoint Security для Linux

Чтобы настроить Kaspersky Endpoint Security для Linux, выполните следующие действия:

1. Добавьте следующие каталоги в список исключений:
   - /opt/kaspersky/ktfs/feeds
   - /opt/kaspersky/ktfs/httpsrv/etc
   - /opt/kaspersky/ktfs/ioc_exports
   - /opt/kaspersky/ktfs/modules/elasticsearch/data
   - /opt/kaspersky/ktfs/var

2. Добавьте следующие приложения в список исключений:

- /opt/kaspersky/ktfs/bin/kl_feed_service
- /opt/kaspersky/ktfs/bin/kl_balancer
- /opt/kaspersky/ktfs/modules/elasticsearch/bin/elasticsearch
- /opt/kaspersky/ktfs/plugins/virus_total/virus_total
- /opt/kaspersky/ktfs/tools/kl_feed_compiler

Более подробные сведения о настройке Kaspersky Endpoint Security для Linux приведены в справке Kaspersky Endpoint Security для Linux.

Часть 2. Интеграция Kaspersky CyberTrace с источником событий

На этом шаге необходимо интегрировать Kaspersky CyberTrace с источником событий. В качестве источника событий может выступать либо одна из SIEM-систем, либо самостоятельный источник событий.

В дополнение к вариантам интеграции, описанным ниже в этом разделе, возможна интеграция и с другими SIEM-системами. Для получения дополнительной информации см. https://support.kaspersky.com/datafeeds.

Интеграция с Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Unified Monitoring and Analysis Platform (KUMA) — это SIEM-система, разработанная «Лабораторией Касперского», которая обеспечивает анализ событий безопасности, генерируемых любыми источниками данных, например приложениями или сетевым оборудованием, в режиме реального времени.

Интеграция доступна только по лицензии Enterprise TIP и для пользователей с ролью «Администратор».

Информация о порядке настройки KUMA для интеграции с Kaspersky CyberTrace приведена в справке Kaspersky Unified Monitoring and Analysis Platform.

Интеграция со Splunk

В этой главе описывается порядок интеграции Kaspersky CyberTrace со Splunk.

Общие схемы интеграции (Splunk)

В этой главе приведено краткое описание порядка интеграции Kaspersky CyberTrace со Splunk.

О схемах интеграции

Возможны две схемы интеграции Kaspersky CyberTrace со Splunk:

- Однокомпонентная схема интеграции

  В однокомпонентной схеме интеграции Kaspersky CyberTrace Service и экземпляр Splunk настраиваются и работают на одном и том же сервере или на разных серверах.

- Распределенная схема интеграции

  В распределенной схеме интеграции Kaspersky CyberTrace Service, Search Head App и Forwarder App устанавливаются в распределенной среде Splunk, при этом служба и приложения настраиваются для взаимодействия друг с другом.

Порядок интеграции Kaspersky CyberTrace со Splunk по однокомпонентной схеме интеграции

Чтобы интегрировать Kaspersky CyberTrace со Splunk по однокомпонентной схеме интеграции, выполните следующие действия:

- Убедитесь, что выполнена установка Kaspersky CyberTrace.

  В однокомпонентной схеме интеграции Kaspersky CyberTrace и экземпляр Splunk устанавливаются на одном и том же сервере или на разных серверах. По умолчанию приложение Kaspersky CyberTrace App для Splunk устанавливается на одном сервере с Kaspersky CyberTrace. Однако рекомендуется устанавливать Kaspersky CyberTrace на отдельный сервер; в этом случае служба Kaspersky CyberTrace Service необходимо настроить во время установки, а приложение Kaspersky CyberTrace для Splunk должно быть настроено на шаге 2 (ниже).

- Шаг 1. Установка Kaspersky CyberTrace App для Splunk.

- Шаг 2 (необязательный). Настройка приложения Kaspersky CyberTrace для Splunk.

  Этот шаг не является обязательным. Если пропустить этот шаг, Kaspersky CyberTrace App для Splunk будет использовать конфигурацию по умолчанию. События в CyberTrace в этом случае отправляться не будут.

  > По умолчанию приложение Kaspersky CyberTrace App для Splunk использует порт 9999 для отправки событий в Kaspersky CyberTrace и порт 9998 для получения событий от Kaspersky CyberTrace. Если эти порты используются другим приложением, необходимо изменить порт либо в Kaspersky CyberTrace App для Splunk, либо в этом другом приложении.

- Шаг 3 (необязательный). Настройка скрипта поиска.

  Этот шаг не является обязательным. Если пропустить этот шаг, скрипт поиска будет использовать конфигурацию по умолчанию.

- Шаг 4. Выполните проверку работоспособности.

  > Перед изменением каких-либо настроек процесса сопоставления необходимо выполнить проверку работоспособности.

Порядок интеграции со Splunk по схеме распределенной интеграции

Чтобы интегрировать Kaspersky CyberTrace со Splunk по схеме распределенной интеграции, выполните следующие действия:

- Убедитесь, что выполнена установка Kaspersky CyberTrace.

  В схеме распределенного развертывания Kaspersky CyberTrace можно установить на один из серверов, на которых уже установлен Forwarder или Indexer, либо на отдельный сервер.

  В схеме распределенного развертывания во время установки необходимо настроить Kaspersky CyberTrace Service для получения событий от других объектов Splunk, таких как форвардеры и индексаторы, и отправлять свои собственные события в тот индексатор, в котором хранится индекс, используемый Kaspersky CyberTrace App для Splunk.

- Шаг 1. Установка Forwarder App и Search Head App.

- Шаг 2. Настройка Forwarder App и Search Head App для взаимодействия друг с другом и пересылки событий в Kaspersky CyberTrace.

- Шаг 3 (необязательный). Настройка скрипта поиска.

  Этот шаг не является обязательным. Если пропустить этот шаг, скрипт поиска будет использовать конфигурацию по умолчанию.

- Шаг 4. Выполните проверку работоспособности.

  Перед изменением каких-либо настроек процесса сопоставления необходимо выполнить проверку работоспособности.

Однокомпонентная схема интеграции (Splunk)

В этом разделе описывается порядок интеграции Kaspersky CyberTrace и Splunk по однокомпонентной схеме интеграции.

Об однокомпонентной схеме интеграции

По умолчанию и Kaspersky CyberTrace Service, и Kaspersky CyberTrace App используют следующую схему интеграции. Это *однокомпонентная схема интеграции*.

О приложениях и службах

Однокомпонентная схема интеграции использует одно приложение и одну службу:

- Kaspersky CyberTrace Service

  Эта служба сопоставляет события Splunk с потоками данных Kaspersky Threat Data Feeds.

  Служба Kaspersky CyberTrace отправляет полученные оповещения в Splunk. Splunk хранит оповещения из службы Kaspersky CyberTrace в индексе `main`.

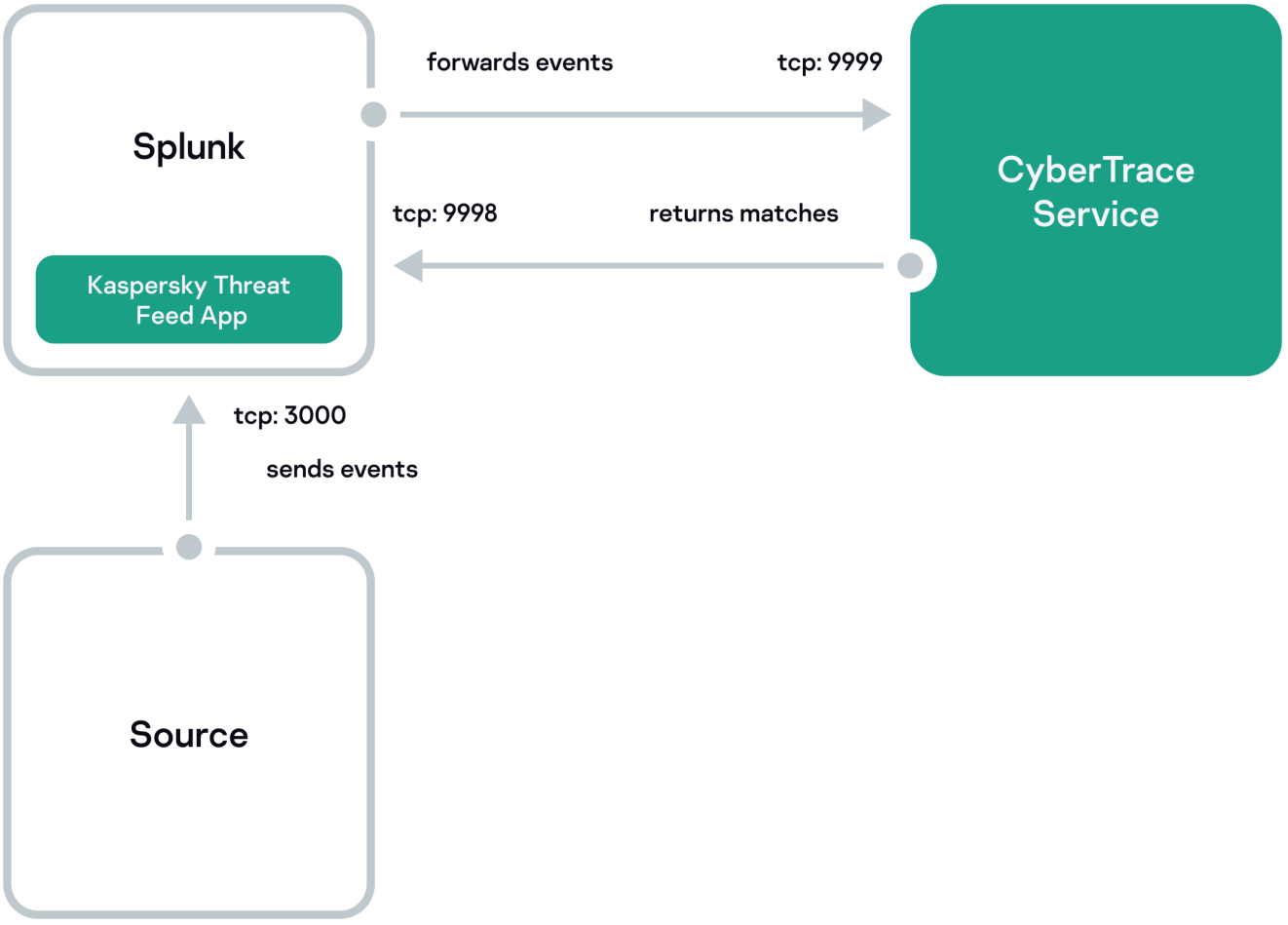
- Kaspersky CyberTrace App

  Это приложение содержит информационные панели приложения Kaspersky CyberTrace App, шаблоны оповещений и скрипт поиска. Приложение также содержит правила парсинга событий Kaspersky CyberTrace Service и правила пересылки событий из Splunk в Kaspersky CyberTrace Service.

Однокомпонентная схема интеграции

В однокомпонентной схеме интеграции приложения Splunk и Kaspersky CyberTrace Service по умолчанию работают на одном сервере (IP-адрес `127.0.0.1`). Kaspersky CyberTrace App принимает входные данные на порт `3000` и перенаправляет их в Kaspersky CyberTrace Service на порте `9999`. После этого Kaspersky CyberTrace Service возвращает результаты сопоставления в Kaspersky CyberTrace App на порт `9998`.

Чтобы установить Kaspersky CyberTrace Service на отдельный сервер, при установке Kaspersky CyberTrace необходимо указать адреса и порты, используемые Kaspersky CyberTrace Service и приложением Kaspersky CyberTrace App.



Однокомпонентная схема интеграции

Формат событий

По умолчанию Kaspersky CyberTrace App и Kaspersky CyberTrace Service получают события в определенном формате:

- Kaspersky CyberTrace Service использует для парсинга событий регулярные выражения из своего конфигурационного файла. Эти регулярные выражения можно просмотреть и настроить на вкладке **Параметры → Источники событий** в веб-интерфейсе Kaspersky CyberTrace. Эти регулярные выражения предназначены для парсинга поступающих данных в определенном формате. Например, регулярное выражение по умолчанию для URL сопоставляет строки, содержащие код протокола (например, `http://` или `https://`). Если URL в событиях, передаваемых устройствами, не содержат указания на протокол, необходимо соответствующим образом изменить регулярное выражение.

- Сценарий поиска, поставляемый с Kaspersky CyberTrace App, отправляет события в Kaspersky CyberTrace Service в формате, с которым могут работать регулярные выражения, используемые в Kaspersky CyberTrace Service. В случае изменения регулярных выражений также необходимо отредактировать скрипт поиска, чтобы в нем использовался формат, соответствующий новым регулярным выражениям.

Шаг 1. Установка Kaspersky CyberTrace (однокомпонентное развертывание)

В этом разделе описывается порядок установки Kaspersky CyberTrace App.

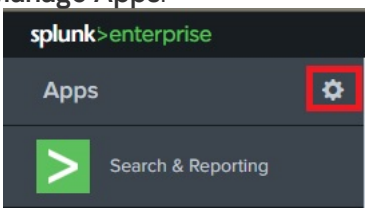
Kaspersky CyberTrace App устанавливается из файла `%service_dir%/integration/splunk/Kaspersky-CyberTrace-App-for-Splunk.tar.gz`.

Установка приложения

Чтобы установить Kaspersky CyberTrace App, выполните следующие действия:

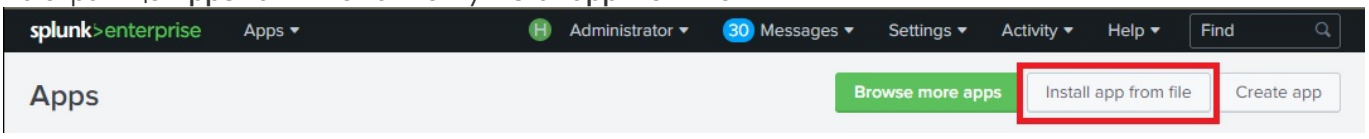
1. В веб-интерфейсе Splunk перейдите на главную страницу.

2. На главной странице нажмите кнопку **Manage Apps**.



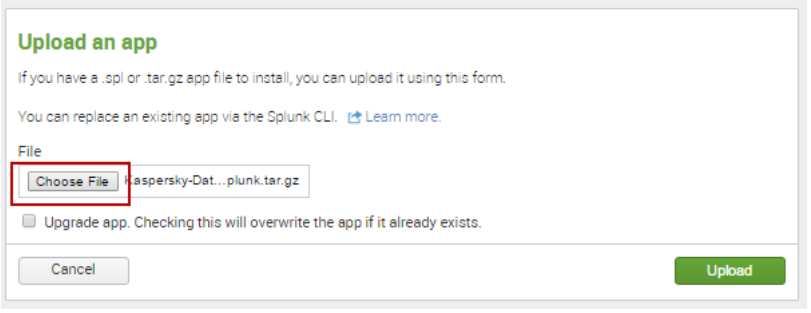
Кнопка **Manage Apps**

3. На странице **Apps** нажмите на кнопку **Install app from file**.



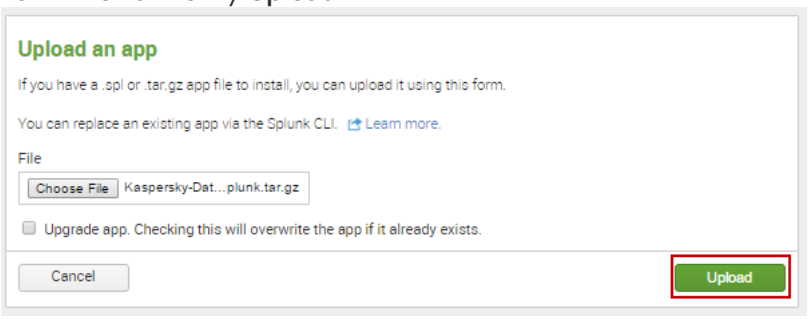
Кнопка **Install app from file**

4. В окне **Upload an app** нажмите **Choose File** и выберите файл Kaspersky CyberTrace App.



Кнопка **Choose File**

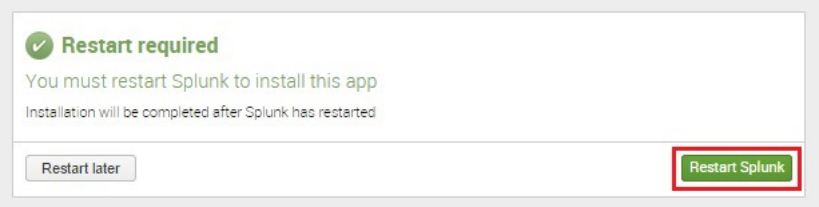
5. В окне **Upload an app** нажмите на кнопку **Upload**.



Кнопка **Upload**

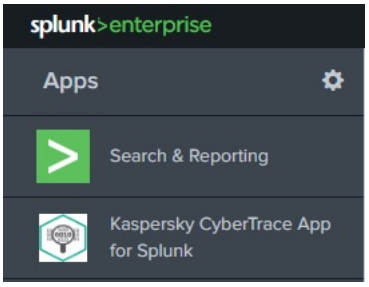
6. В окне **Restart required** нажмите кнопку **Restart Splunk**.

   В некоторых версиях Splunk этот шаг можно пропустить. Если в Splunk не отображается окно **Restart required**, пропустите этот шаг.



Кнопка **Restart Splunk**

7. При повторном запуске Splunk откроется страница **Apps** с информацией об успешной установке Kaspersky CyberTrace App. Kaspersky CyberTrace App появится в списке приложений на главной странице Splunk.



Kaspersky CyberTrace App для Splunk в списке приложений

Шаг 2 (необязательный). Настройка приложения Kaspersky CyberTrace App (однокомпонентное развертывание)

Kaspersky CyberTrace App считывает свои параметры из конфигурационных файлов. Эти конфигурационные файлы определяют настройки ввода и вывода и формат событий, используемый Kaspersky CyberTrace App.

После внесения изменений в конфигурационные файлы Kaspersky CyberTrace App необходимо перезапустить Splunk.

Изменять следует только те конфигурационные файлы Kaspersky CyberTrace App, которые описаны в этом разделе. Изменение других конфигурационных файлов Kaspersky CyberTrace App может привести к непредсказуемому поведению.

О конфигурационных файлах

Для настройки Kaspersky CyberTrace App можно использовать следующие конфигурационные файлы (`$SPLUNK_HOME` соответствует каталогу установки Splunk):

- `$SPLUNK_HOME/etc/apps/Kaspersky-CyberTrace-App-for-Splunk/default/commands.conf`

  В этом конфигурационном файле задается команда для скрипта поиска.

- `$SPLUNK_HOME/etc/apps/Kaspersky-CyberTrace-App-for-Splunk/default/inputs.conf`

  В этом конфигурационном файле задаются настройки ввода Kaspersky CyberTrace App. Сюда входят порты и адреса для приема данных из источников событий и для входящих событий обнаруженных киберугроз от Kaspersky CyberTrace Service.

- `$SPLUNK_HOME/etc/apps/Kaspersky-CyberTrace-App-for-Splunk/default/outputs.conf`

  В этом конфигурационном файле задаются параметры пересылки событий в Kaspersky CyberTrace Service.

- `$SPLUNK_HOME/etc/apps/Kaspersky-CyberTrace-App-for-Splunk/default/props.conf`

  В этом конфигурационном файле задаются параметры обработки входных данных.

- `$SPLUNK_HOME/etc/apps/Kaspersky-CyberTrace-App-for-Splunk/default/savedsearches.conf`

  В этом конфигурационном файле задаются параметры для шаблонов оповещени.

Файл commands.conf по умолчанию

В этом файле задается скрипт поиска, который Kaspersky CyberTrace App будет использовать при выполнении пользователем команды `klsearch`.

Ниже показано содержимое конфигурационного файла commands.conf по умолчанию.

```
[klsearch]
filename = kl_search.py
```

Файл inputs.conf по умолчанию

В этом конфигурационном файле задаются настройки ввода для Kaspersky CyberTrace App.

По умолчанию Kaspersky CyberTrace App работает следующим образом:

- События обнаруженных киберугроз из Kaspersky CyberTrace Service принимаются на адрес с портом `:9998`.
- Данные из источников принимаются на адрес с портом `:3000` (а затем пересылаются на адрес `127.0.0.1:9999`, заданный в файле outputs.conf).

Ниже показано содержимое конфигурационного файла inputs.conf по умолчанию.

```
[tcp://:9998]
_INDEX_AND_FORWARD_ROUTING=local
connection_host = dns
index = main
sourcetype = kl_cybertrace_events
source = tcp:9998
disabled = false

[tcp://:3000]
_TCP_ROUTING = service9999
```

Файл outputs.conf по умолчанию

В этом конфигурационном файле задаются настройки вывода для Kaspersky CyberTrace App.

По умолчанию Kaspersky CyberTrace App пересылает данные с адреса с портом `:3000` в Kaspersky CyberTrace Service по адресу `127.0.0.1:9999`. Входной порт (`:3000`) задается в файле inputs.conf.

Ниже показано содержимое конфигурационного файла outputs.conf по умолчанию.

```
[tcpout]
defaultGroup = noforward
disabled = false

[indexAndForward]
index=true

[tcpout:service9999]
disabled=false
server = 127.0.0.1:9999
sendCookedData = false
```

Файл props.conf по умолчанию

Этот файл определяет, как Splunk обрабатывает входящие данные.

По умолчанию Kaspersky CyberTrace App работает следующим образом:

- Определяется способ извлечения меток времени из входящих данных.
- Определяется разделитель (перенос строки) между событиями для входящих данных.

  Например, если входящие данные состоят из последовательности «`%data_1%\n\n%data_2%`», а перенос строки состоит из одного или нескольких символов `\n`, Splunk разбивает эту последовательность на два события (`%data_1%` и `%data_2%`).

Ниже показано содержимое конфигурационного файла props.conf по умолчанию.

```
[source::tcp:3000]
TIME_PREFIX = ^
MAX_TIMESTAMP_LOOKAHEAD = 17
TIME_FORMAT = %b %d %H:%M:%S
LINE_BREAKER = ([\n]+)
SHOULD_LINEMERGE = false

[source::tcp:9998]
TIME_PREFIX = ^
MAX_TIMESTAMP_LOOKAHEAD = 17
TIME_FORMAT = %b %d %H:%M:%S
LINE_BREAKER = ([\n]+)
SHOULD_LINEMERGE = false
```

Можно изменить порт, который Kaspersky CyberTrace должен прослушивать в ожидании входящих событий от источника, или добавить новые источники событий.

Чтобы изменить порт, который Kaspersky CyberTrace прослушивает для получения входящих событий от источника, выполните следующие действия:

1. В файле inputs.conf измените номер порта по умолчанию `3000` на требуемый номер порта.

   Например, если требуется изменить порт `3000` на `3010`, запись в файле inputs.conf будет выглядеть следующим образом:

   ```
   [tcp://:3010]
   _TCP_ROUTING = service9999
   ```

2. В файле props.conf также измените порт 3000, заданный по умолчанию, на требуемый номер порта.

   Например, если требуется изменить порт `3000` на `3010`, запись в файле props.conf будет выглядеть следующим образом:

   ```
   [source::tcp:3010]
   TIME_PREFIX = ^
   MAX_TIMESTAMP_LOOKAHEAD = 17
   TIME_FORMAT = %b %d %H:%M:%S
   LINE_BREAKER = ([\n]+)
   SHOULD_LINEMERGE = false
   ```

3. Перезапустите Splunk.

Чтобы добавить новый источник событий, выполните следующие действия:

1. В файле inputs.conf укажите новый источник событий, использующий правило маршрутизации TCP `service9999`.

   Все данные из этого источника будут пересылаться в Kaspersky CyberTrace Service.

2. В файле props.conf укажите способ обработки данных из этого источника.

3. Перезапустите Splunk.

Убедитесь, что данные из нового источника событий успешно обрабатываются регулярными выражениям, используемыми Kaspersky CyberTrace.

Ниже приведен пример добавления адреса `:3001` в качестве источника событий; в примере задается, что данные с адреса `:3001` должны обрабатываться, как и другие входные данные в схеме интеграции по умолчанию (в этой схеме форвардер, индексатор и search head установлены на одном сервере).

```
# в inputs.conf
[tcp://:3001]
_TCP_ROUTING = service9999

# в props.conf
[source::tcp:3001]
TIME_PREFIX = ^
MAX_TIMESTAMP_LOOKAHEAD = 17
TIME_FORMAT = %b %d %H:%M:%S
LINE_BREAKER = ([\n]+)
SHOULD_LINEMERGE = false
```

Изменение адреса и порта для данных из Kaspersky CyberTrace Service

По умолчанию в Kaspersky CyberTrace App настроено получение данных от Kaspersky CyberTrace Service на порт `9998` по любому доступному адресу. Это задается в конфигурационном файле inputs.conf Kaspersky CyberTrace App. Если требуется получать данные от Kaspersky CyberTrace Service только по определенному адресу и на определенный порт (например, если Splunk имеет доступ к нескольким сетевым интерфейсам), отредактируйте файл inputs.conf соответствующим образом.

Чтобы задать адрес и порт, где Kaspersky CyberTrace App должен получать данные от Kaspersky CyberTrace Service, необходимо задать следующие правила:

- Если Kaspersky CyberTrace Service и Splunk установлены на одном сервере, укажите порт, на который Kaspersky CyberTrace App должен получать данные от Kaspersky CyberTrace Service, в следующем формате:

  `[tcp://127.0.0.1:<порт>]`

- Если Kaspersky CyberTrace Service и Splunk установлены на разных серверах, укажите адрес и порт, на которые Kaspersky CyberTrace App должен получать данные от Kaspersky CyberTrace Service, в следующем формате:

  `[tcp://<адрес>:<порт>]`

- Чтобы указать, что Kaspersky CyberTrace App должен получать данные от Kaspersky CyberTrace Service по любому доступному адресу, используйте следующий формат:

  `[tcp://:<порт>]`

  Обратите внимание, что этот формат может повлиять на безопасность, поскольку Kaspersky CyberTrace App будет получать информацию на указанный порт со всех доступных сетевых интерфейсов.

В приведенных выше примерах формата `<адрес>` и `<порт>` — это IP-адрес и порт, которые Kaspersky CyberTrace App должен прослушивать для получения входящих данных от Kaspersky CyberTrace Service.

Возможно, также потребуется изменить адреса и порты для исходящих событий, используемые в Kaspersky CyberTrace.

Ниже приведены примеры указания адреса и порта для получения данных от Kaspersky CyberTrace Service.

В следующем примере Kaspersky CyberTrace Service и Splunk расположены на одном сервере. Kaspersky CyberTrace App получает события обнаруженных киберугроз на порту `9998` того же сервера.

```
[tcp://127.0.0.1:9998]
_INDEX_AND_FORWARD_ROUTING=local
connection_host = dns
index = main
sourcetype = kl_cybertrace_events
source = tcp:9998
disabled = false
```

В следующем примере Kaspersky CyberTrace Service и Splunk расположены на разных серверах. Kaspersky CyberTrace App получает события обнаруженных киберугроз от Kaspersky CyberTrace Service по адресу `192.0.2.42:9997`.

```
[tcp://192.0.2.42:9997]
_INDEX_AND_FORWARD_ROUTING=local
connection_host = dns
index = main
sourcetype = kl_cybertrace_events
source = tcp:9997
disabled = false
```

В следующем примере Kaspersky CyberTrace App получает события обнаруженных киберугроз от Kaspersky CyberTrace Service на порт `3000` любого доступного адреса.

```
[tcp://:3000]
_INDEX_AND_FORWARD_ROUTING=local
connection_host = dns
index = main
sourcetype = kl_cybertrace_events
source = tcp:3000
disabled = false
```

Настройка шаблонов оповещений

В Kaspersky CyberTrace входит несколько шаблонов оповещений, которые можно использовать и настраивать на информационной панели **Alerts**.

Доступны следующие шаблоны оповещений:

- Оповещение «Matches»

  Это оповещение срабатывает, если за последние 24 часа были обнаружены киберугрозы при сопоставлении с потоками данных об угрозах Kaspersky Threat Data Feeds.

- Оповещение «No Matches»

  Это оповещение срабатывает, если за последние 24 часа не было обнаружено киберугроз при сопоставлении с потоками данных об угрозах Kaspersky Threat Data Feeds.

- Оповещение «Emergency»

  Это предупреждение срабатывает, если в течение одной минуты было обнаружено 5000 совпадений при сопоставлении с потоками данных об угрозах Kaspersky Threat Data Feeds.

- Оповещение «Service Unavailable»

  Это оповещение срабатывает в случае недоступности Kaspersky CyberTrace Service.

- Оповещение «Service Started»

  Это оповещение срабатывает при запуске Kaspersky CyberTrace Service.

Ниже приведены настройки Kaspersky CyberTrace App по умолчанию:

- Все оповещения, входящие в Kaspersky CyberTrace App, включены.

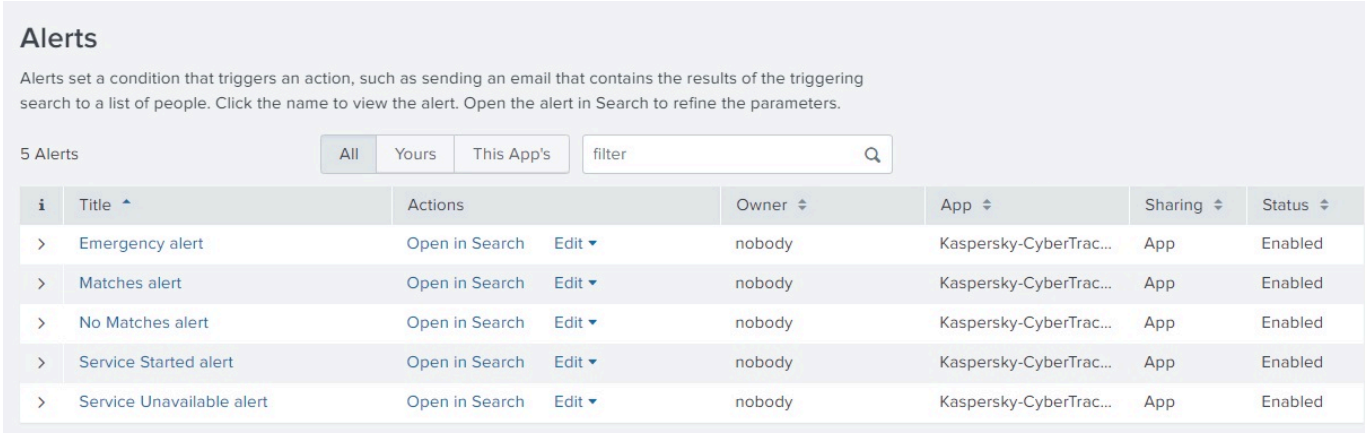
  Их можно выключить на информационной панели **Alerts**.

- Для всех оповещений задано действие «Add to Triggered Alerts».

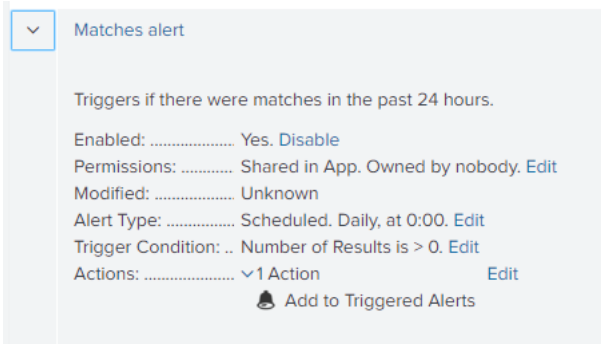
  Splunk отображает оповещение в разделе «Triggered Alerts».

Чтобы включить уведомления по электронной почте для оповещений, выполните следующие действия:

1. В Kaspersky CyberTrace App откройте вкладку **Alerts**.

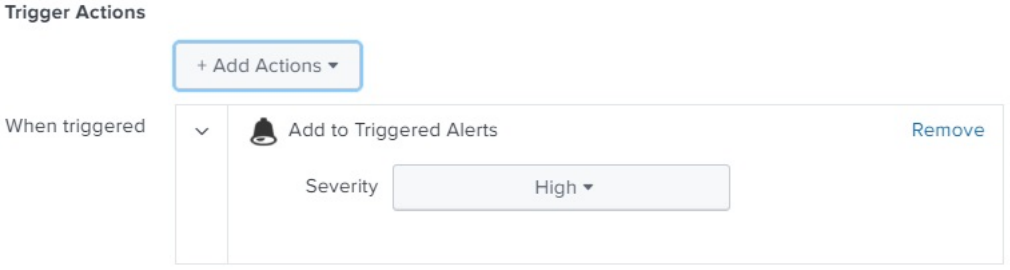


2. Разверните параметры оповещения, которое требуется настроить.

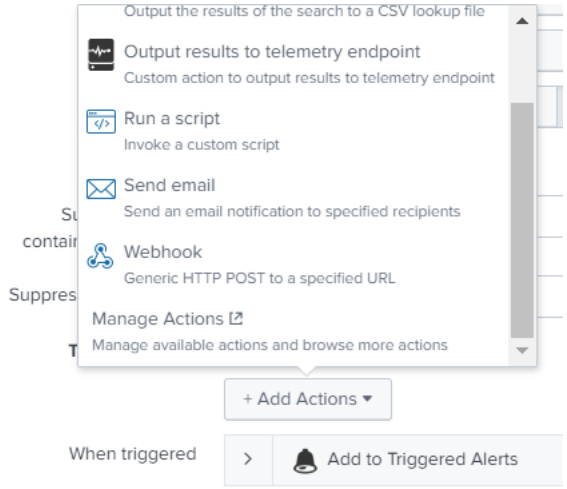


3. Найдите поле **Actions** и нажмите кнопку **Edit**.

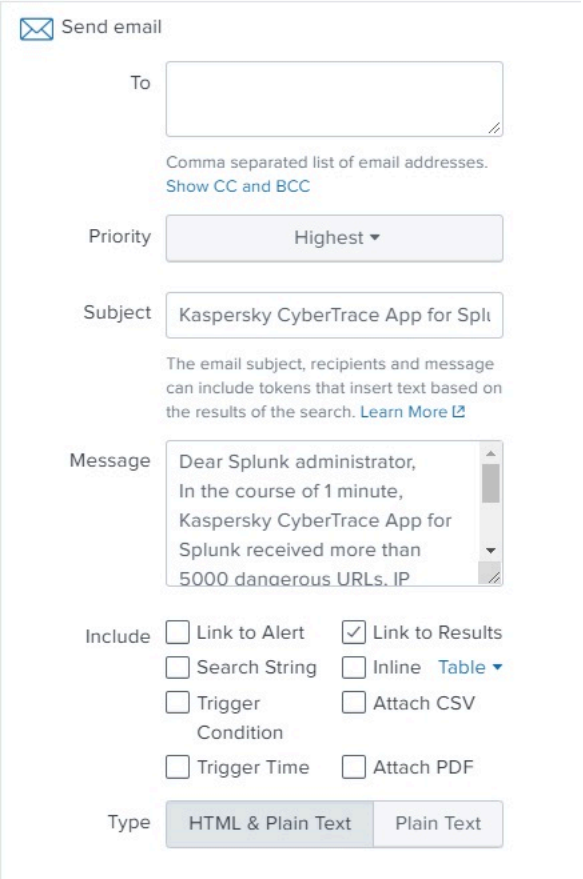
4. В разделе **Trigger Actions** нажмите на кнопку **Add Actions**.



5. Выберите вариант **Send email** из списка.



6. Введите параметры электронной почты и сохраните изменения.



Шаг 3 (необязательный). Настройка скрипта поиска (однокомпонентное развертывание)

Скрипт поиска используется для сопоставления отдельных URL, IP-адресов и хешей с потоками данных об угрозах Kaspersky Threat Data Feeds. Скрипт можно вызвать на вкладке **Indicators lookup** в Kaspersky CyberTrace App.

Чтобы настроить скрипт поиска, выполните следующие действия:

1. В Kaspersky CyberTrace App перейдите на вкладку **Indicators lookup**.

2. Задайте строки подключения к Kaspersky CyberTrace:

   - В поле **Kaspersky CyberTrace address** укажите IP-адрес Kaspersky CyberTrace.

   - В поле **Kaspersky CyberTrace port** укажите порт, используемый Kaspersky CyberTrace.

Скрипт готов к использованию.

Шаг 4. Проверка работоспособности (Splunk, однокомпонентная схема интеграции)

В этом разделе описывается порядок проверки возможностей Kaspersky CyberTrace с помощью проверки работоспособности.

Перед изменением каких-либо настроек процесса сопоставления необходимо выполнить проверку работоспособности.

О проверке работоспособности

Проверка работоспособности — это процедура, позволяющая проверить возможности Kaspersky CyberTrace и убедиться в корректности интеграции.

В ходе проверки проверяется, поступают ли события из Splunk в Kaspersky CyberTrace Service, поступают ли события из Kaspersky CyberTrace Service в Splunk, и корректно ли проходит парсинг событий в Kaspersky CyberTrace Service с использованием регулярных выражений.

В этом разделе описывается сценарий проверки для схемы интеграции по умолчанию (в этой схеме форвардер, индексатор и search head установлены на одном сервере), однако проверку работоспособности также можно использовать после внесения изменений в параметры конфигурации для проверки корректности работы Kaspersky CyberTrace и SIEM-системы.

Файл проверки работоспособности

Файл проверки работоспособности — это файл `%service_dir%/verification/kl_verification_test_cef.txt`. В этом файле содержится набор событий с URL, IP-адресами и хешами.

Сценарий проверки работоспособности (краткое описание)

Чтобы выполнить проверку работоспособности, выполните следующие действия:

1. Укажите адрес Splunk Forwarder в конфигурационном файле утилиты Log Scanner.
2. Отправьте проверочный файл в Kaspersky CyberTrace Service с помощью утилиты Log Scanner.
3. Сравните результаты проверки работоспособности с целевыми числами, отображаемыми на информационной панели **Kaspersky CyberTrace Matches**.
4. Выполните самостоятельную диагностику.

   Самостоятельная диагностика — это автоматический тест потока данных об угрозах, выполняемый приложением Kaspersky CyberTrace App.
5. Если требуется, можно также очистить Splunk от событий, которые были получены во время выполнения проверки работоспособности.

Сценарий проверки работоспособности

Сценарий проверки работоспособности состоит из следующих этапов:

1-й этап. Указание адреса Splunk Forwarder в конфигурационном файле утилиты Log Scanner.

Укажите адрес и порт, которые прослушивает Splunk Forwarder, в элементе `Connection` конфигурационного файла Log Scanner.

2-й этап. Отправка проверочного файла в Splunk Forwarder

Проверочный файл необходимо отправить в Splunk Forwarder с помощью утилиты Log Scanner.

Перед отправкой файла убедитесь, что Kaspersky CyberTrace Service запущена.

Следующие команды отправляют содержимое файла `kl_verification_test_cef.txt` в Kaspersky CyberTrace Service:

- В ОС Linux: `./log_scanner -p ../verification/kl_verification_test_cef.txt`
- В ОС Windows: `log_scanner.exe -p ..\verification\kl_verification_test_cef.txt`

Получив данные от Log Scanner, Splunk Forwarder отправляет результаты проверки в Kaspersky CyberTrace. Обнаруженные индикаторы из проверочного файла будут отправлены обратно в Splunk Forwarder. Адрес Splunk Forwarder указывается в настройках служб Kaspersky CyberTrace. Также этот адрес указывается при установке или изменении конфигурации Kaspersky CyberTrace.

3-й этап. Контроль результатов проверки работоспособности

На этом шаге необходимо проверить правильность обработки URL, IP-адресов и хешей в приложении Kaspersky CyberTrace App.

IP-адреса из тестовых записей, используемых для проверки, не отображаются на карте **Location of matched IPs**. Для проверки работы карты рекомендуется использовать другие записи из базы данных Kaspersky CyberTrace. Записи, содержащие IP-адреса, можно получить на вкладке **Индикаторы** в веб-интерфейсе Kaspersky CyberTrace.

Чтобы проконтролировать результаты проверки работоспособности, выполните следующие действия:

1. В приложении Kaspersky CyberTrace App на панели навигации выберите **Kaspersky CyberTrace Matches**.

   Откроется информационная панель **Kaspersky CyberTrace Matches**.

2. Сравните номера на панели **Matches by eventName** с номерами обнаруженных объектов в таблице, приведенной ниже.

   Результаты проверки работоспособности зависят от используемых потоков данных об угрозах. В следующей таблице приведены целевые номера для проверки работоспособности при использовании всех коммерческих потоков данных об угрозах.

Результаты проверки работоспособности (коммерческие потоки данных об угрозах)

Используемый поток данных об угрозах	Значение eventName	Обнаруженные объекты
Malicious URL Data Feed	KL_Malicious_URL	http://fakess123.nu http://badb86360457963b90faac9ae17578ed.com
Phishing URL Data Feed	KL_Phishing_URL	http://fakess123ap.nu http://e77716a952f640b42e4371759a661663.com
Botnet C&C URL Data Feed	KL_BotnetCnC_URL	http://fakess123bn.nu http://a7396d61caffe18a4cffbb3b428c9b60.com
IP Reputation Data Feed	KL_IP_Reputation	192.0.2.0 192.0.2.3

Malicious Hash Data Feed	KL_Malicious_Hash_MD5	FEAF2058298C1E174C2B79AFFC7CF4DF 44D88612FEA8A8F36DE82E1278ABB02F C912705B4BBB14EC7E78FA8B370532C9
Mobile Malicious Hash Data Feed	KL_Mobile_Malicious_Hash_MD5	60300A92E1D0A55C7FDD360EE40A9DC1
Mobile Botnet C&C URL Data Feed	KL_Mobile_BotnetCnC_Hash_MD5	001F6251169E6916C455495050A3FB8D
Mobile Botnet C&C URL Data Feed	KL_Mobile_BotnetCnC_URL	http://sdfed7233dsfg93acvbhl.su/steallallsms.php
Ransomware URL Data Feed	KL_Ransomware_URL	http://fakess123r.nu http://fa7830b4811fbef1b187913665e6733c.com
APT URL Data Feed	KL_APT_URL	http://b046f5b25458638f6705d53539c79f62.com
APT Hash Data Feed	KL_APT_Hash_MD5	7A2E65A0F70EE0615EC0CA34240CF082
APT IP Data Feed	KL_APT_IP	192.0.2.4
IoT URL Data Feed	KL_IoT_URL	http://e593461621ee0f9134c632d00bf108fd.com/.i
ICS Hash Data Feed	KL_ICS_Hash_MD5	7A8F30B40C6564EFF95E678F7C43346C

В следующей таблице приведены целевые номера для проверки работоспособности при использовании только демонстрационных потоков данных об угрозах.

Результаты проверки работоспособности (демонстрационные потоки данных об угрозах)

Используемый поток данных об угрозах	Значение eventName	Обнаруженные объекты
DEMO Botnet_CnC_URL_Data_Feed	KL_BotnetCnC_URL	http://5a015004f9fc05290d87e86d69c4b237.com http://fakess123bn.nu
DEMO IP_Reputation_Data_Feed	KL_IP_Reputation	192.0.2.1 192.0.2.3
DEMO Malicious_Hash_Data_Feed	KL_Malicious_Hash_MD5	776735A8CA96DB15B422879DA599F474 FEAF2058298C1E174C2B79AFFC7CF4DF 44D88612FEA8A8F36DE82E1278ABB02F

4-й этап. Выполнение самостоятельной диагностики

Самостоятельная диагностика — это автоматический тест потока данных об угрозах, выполняемый приложением Kaspersky CyberTrace App с использованием скрипта поиска. Необходимо убедиться в корректности результатов этого теста.

Чтобы выполнить самостоятельную диагностику, выполните следующие действия:

1. В приложении Kaspersky CyberTrace App на панели навигации выберите **Kaspersky CyberTrace Status**.

   Откроется информационная панель **Kaspersky CyberTrace Status**.

2. На панели **Self-test** проверьте значения `status` для всех используемых потоков данных об угрозах:

   - Если используются только демонстрационные потоки данных, для демонстрационных потоков данных должно отображаться значение `OK`, а для всех остальных потоков данных должно отображаться значение `FALSE`.

   - Если используются коммерческие потоки данных, для всех используемых потоков данных должно отображаться значение `OK`. Для всех остальных потоков данных, включая демонстрационные, должно отображаться значение `FALSE`.

На следующем рисунке показан пример результатов самостоятельной диагностики для коммерческих потоков данных об угрозах. В этом примере используются все коммерческие потоки данных об угрозах, а демонстрационные потоки данных об угрозах не используются. Как и ожидалось, значение для демонстрационных потоков данных об угрозах — `FALSE`.


Self-test

feed	status
Malicious_URL_Data_Feed	OK
P-SMS_Trojan_Data_Feed	OK
Ransomware_URL_Data_Feed	OK
Malicious_Hash_Data_Feed	OK
DEMO Botnet_C&C_URL_Data_Feed	FALSE
Phishing_URL_Data_Feed	OK
Mobile_Malicious_Hash_Data_Feed	OK
DEMO Malicious_Hash_Data_Feed	FALSE
DEMO IP_Reputation_Data_Feed	FALSE
Botnet_C&C_URL_Data_Feed	OK

« prev 1 2 next »

Результаты самостоятельной диагностики

5-й этап (необязательный). Очистка Splunk от событий, полученных при выполнении проверки работоспособности

Чтобы очистить Splunk от событий, полученных от Kaspersky CyberTrace при выполнении проверки работоспособности, выполните следующие действия:

1. На информационной панели **Search** в веб-интерфейсе Splunk нажмите кнопку **Search & Reporting**, чтобы запустить приложение «Search & Reporting».

2. Удалите события из Kaspersky CyberTrace:

   > Удаление событий из индекса main возможно только под учетной записью пользователя с ролью can_delete. Чтобы добавить эту роль в учетную запись пользователя, необходимо выбрать **Settings** → **Roles** в главном меню Splunk.

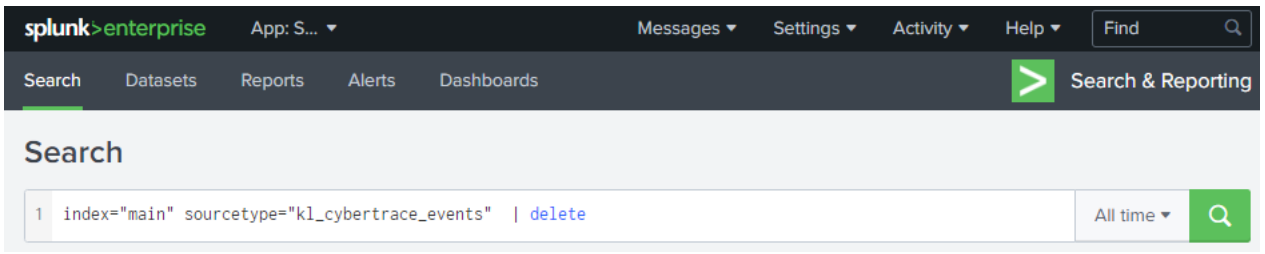
   a. В поле **Search** введите следующую команду:

   ```
   index="main" sourcetype="kl_cybertrace_events" | delete
   ```

   b. Нажмите на кнопку **All time** рядом с полем **Search**.

   Если у кнопки другое название, нажмите на нее и в раскрывающемся списке выберите **All time**.

   c. Нажмите на кнопку **Search** ( ).



Приложение «Search & Reporting»

Распределенная схема интеграции (Splunk)

В этом разделе описывается порядок интеграции Kaspersky CyberTrace и Splunk по распределенной схеме интеграции.

О распределенной схеме интеграции

Kaspersky CyberTrace поддерживает распределенные среды Splunk. Схема интеграции для распределенных сред Splunk называется *распределенной схемой интеграции*.

О приложениях и службах, используемых в распределенной схеме интеграции

В распределенной схеме интеграции Kaspersky CyberTrace разделяется на два приложения и одну службу:

- Kaspersky CyberTrace Service

  Эта служба сопоставляет события Splunk с потоками данных Kaspersky Threat Data Feeds.

  Kaspersky CyberTrace Service отправляет полученные оповещения в единственный индексатор, который ведет индекс оповещений, полученных от Kaspersky CyberTrace.

  Эта служба может быть установлена на отдельном сервере.

- Kaspersky CyberTrace App Search Head (или Search Head App)

  Это приложение содержит информационные панели Kaspersky CyberTrace App, шаблоны оповещений и скрипт поиска.

  Это приложение предназначено для установки в экземпляре Splunk, выступающем в качестве search head и отправляющем поисковые запросы в индексатор, который ведет индекс оповещений, полученных от Kaspersky CyberTrace.

- Kaspersky CyberTrace App Forwarder (или Forwarder App)

  Это приложение содержит правила пересылки событий из Splunk в Kaspersky CyberTrace Service. Оно также получает события из Kaspersky CyberTrace Service.

  Это приложение предназначено для установки в экземплярах Splunk, которые должны пересылать события в Kaspersky CyberTrace Service.

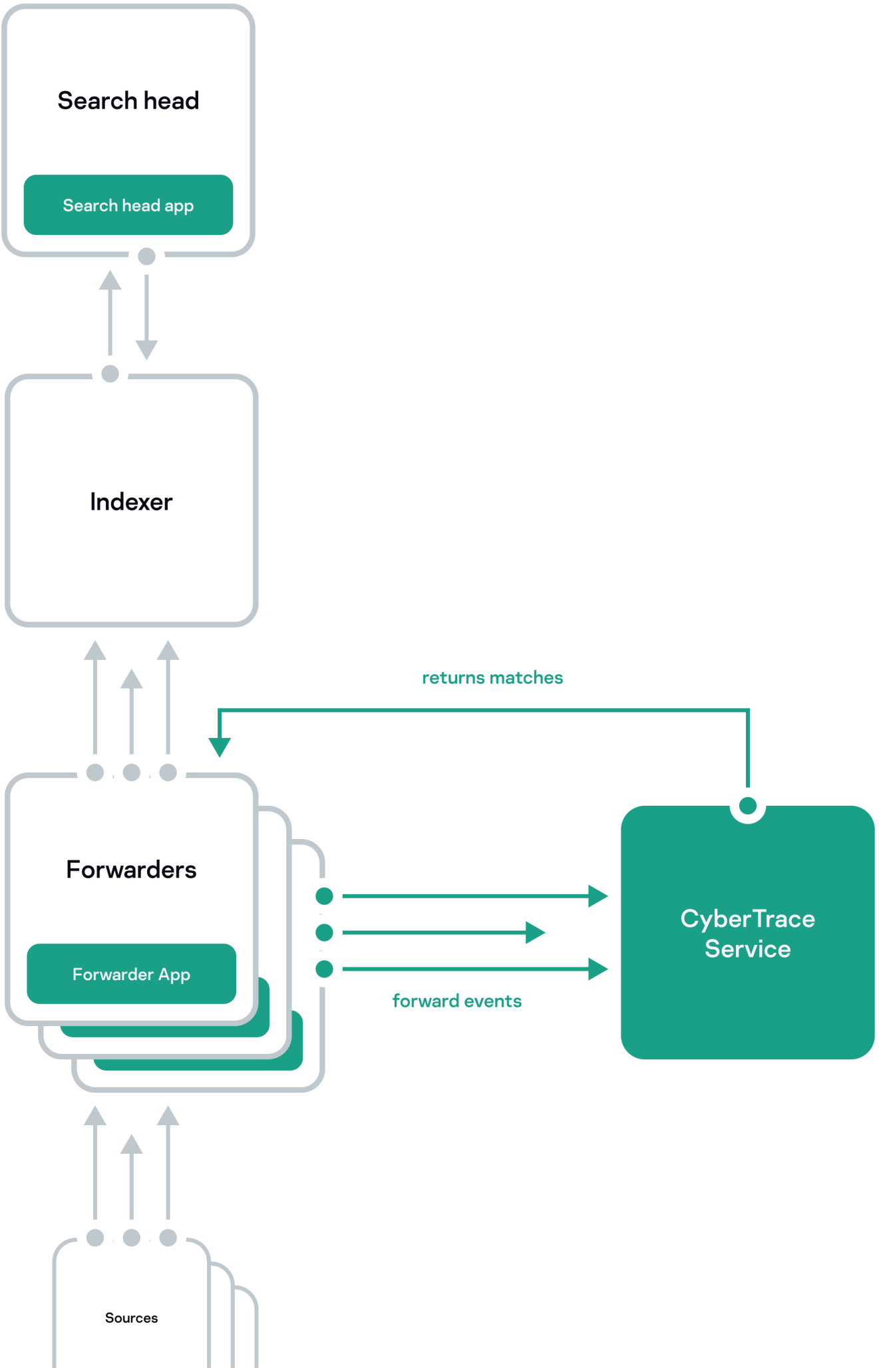
  Kaspersky CyberTrace App Forwarder разделяется на два приложения в зависимости от типа Splunk Forwarder, используемого в распределенной схеме интеграции:

  - App for Heavy Forwarder
  - App for Universal Forwarder

О вариантах схемы интеграции

Следующие варианты схемы распределенной схемы интеграции демонстрируют общий подход к интеграции Kaspersky CyberTrace с распределенной средой Splunk. В зависимости от того, как организована распределенная среда Splunk, может потребоваться изменить или комбинировать эти варианты.

Вариант с одним индексатором и несколькими форвардерами


Search head
Search head app
Indexer
returns matches
Forwarders
Forwarder App
forward events
CyberTrace Service
Sources



Один индексатор, несколько форвардеров

В варианте с *одним индексатором и несколькими форвардерами* несколько Heavy Forwarder или Universal Forwarder получают и пересылают события непосредственно в Kaspersky CyberTrace Service. Они должны использовать Forwarder App (для соответствующего типа Forwarder). Один из Forwarder'ов получает результаты сопоставления от Kaspersky CyberTrace Service. Форвардер отправляет результаты сопоставления в индексатор, который сохраняет их в индексе main, используемом Kaspersky CyberTrace для Splunk Search Head App.

Вариант с несколькими индексаторами и несколькими форвардерами

В варианте с *несколькими индексаторами и несколькими форвардерами* несколько Heavy Forwarder или Universal Forwarder получают и пересылают события непосредственно в Kaspersky CyberTrace Service. Они должны использовать Forwarder App (для соответствующего типа Forwarder). Один из Forwarder'ов получает результаты сопоставления от Kaspersky CyberTrace Service. Форвардер отправляет совпадения в индексаторы, которые сохраняют их в индексе main, используемом Kaspersky CyberTrace App.

Порты и адреса по умолчанию

По умолчанию Forwarder App и Kaspersky CyberTrace Service настроены на использование определенных адресов и портов для пересылки событий и получения результатов сопоставления. Эти адреса и порты необходимо изменить в соответствии со структурой используемой распределенной среды Splunk.

Необходимо изменить адреса и порты по умолчанию, которые используются в Forwarder App и Kaspersky CyberTrace Service.

По умолчанию Forwarder App:

- Принимает события на порте `:3000`.
- Получает события от Kaspersky CyberTrace на порт `:9998`. Эти события хранятся в индексе `main`.
- Пересылает события на `127.0.0.1:9999`.

По умолчанию Kaspersky CyberTrace Service работает следующим образом:

- Получает события на `127.0.0.1:9999`.
- Отправляет собственные оповещения на `127.0.0.1:9998`.

Формат событий

По умолчанию Kaspersky CyberTrace App и Kaspersky CyberTrace Service настроены для получения событий в определенном формате:

- Kaspersky CyberTrace Service выполняет парсинг событий с помощью регулярных выражений, заданных в его конфигурационном файле (регулярные выражения также отображаются в веб-интерфейсе Kaspersky CyberTrace). Эти регулярные выражения предназначены для поступающих данных в определенном формате. Например, регулярное выражение по умолчанию для URL сопоставляет URL вместе с протоколом (например, HTTP, HTTPS). Если URL в событиях, генерируемых устройствами, не включают протокол, измените регулярное выражение соответствующим образом.

- Сценарий поиска, поставляемый с Kaspersky CyberTrace App (или Search Head App в случае распределенной схемы интеграции), отправляет события в Kaspersky CyberTrace Service в формате, соответствующем регулярным выражениям, которые использует Kaspersky CyberTrace Service.

Шаг 1. Установка приложений Forwarder App и Search Head App

При использовании распределенной схемы развертывания необходимо установить Forwarder App и Search Head App в соответствии со структурой используемой распределенной среды Splunk. Подробнее о выборе серверов для установки приложений сообщается в разделе, посвященном распределенной схеме интеграции.

Forwarder App устанавливается из следующих файлов:

- Для Heavy Forwarder: `%service_dir%/integration/splunk/Kaspersky-CyberTrace-App-for-Splunk_Forwarder.tar.gz`

- Для Universal Forwarder: `%service_dir/integration/splunk/Kaspersky-CyberTrace-App-for-Splunk_Universal-Forwarder.tar.gz`

Search Head App устанавливается из файла `%service_dir%/integration/splunk/Kaspersky-CyberTrace-App-for-Splunk_Search-Head.tar.gz`.

Установка приложений

Приложение Forwarder App for Heavy Forwarder и Search Head App устанавливаются из веб-интерфейса Splunk. Их процессы установки различаются только именем файла приложения.

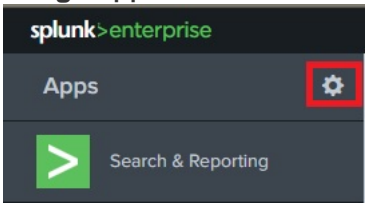
Forwarder App for Universal Forwarder устанавливается непосредственно на хост, поскольку Splunk Universal Forwarder не имеет веб-интерфейса Splunk.

Чтобы установить Forwarder App for Heavy Forwarder или Search Head App, выполните следующие действия:

1. Откройте веб-интерфейс Splunk для экземпляра Splunk, на который требуется установить приложение.

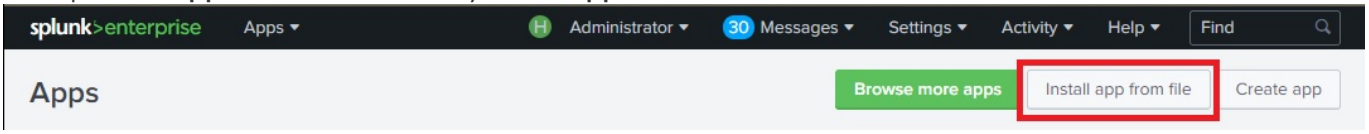
2. В веб-интерфейсе Splunk перейдите на главную страницу.

3. На главной странице нажмите кнопку **Manage Apps**.



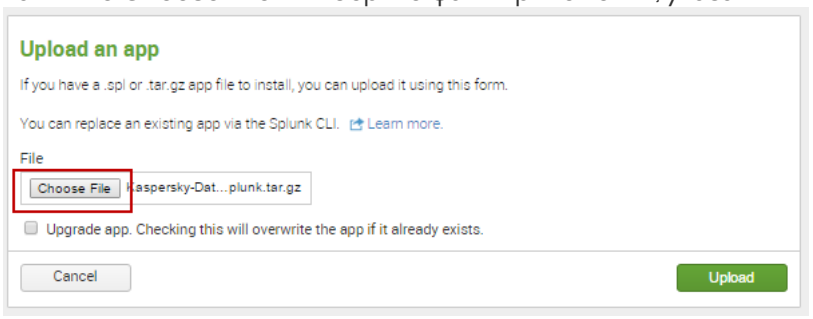
Кнопка **Manage Apps**

4. На странице **Apps** нажмите на кнопку **Install app from file**.



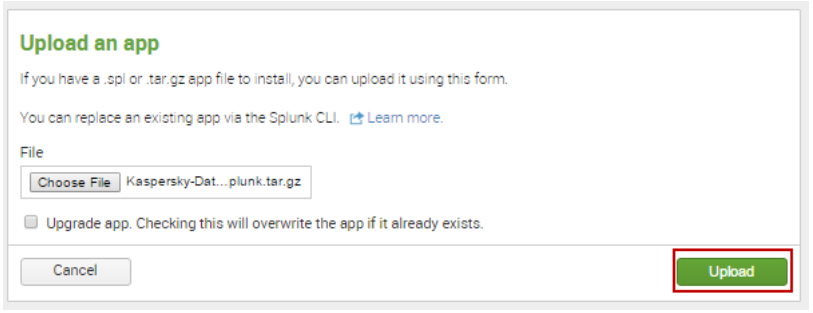
Кнопка **Install app from file**

5. В окне **Upload an app** нажмите **Choose File** и выберите файл приложения, указанный выше в этом разделе.



Кнопка **Choose File**

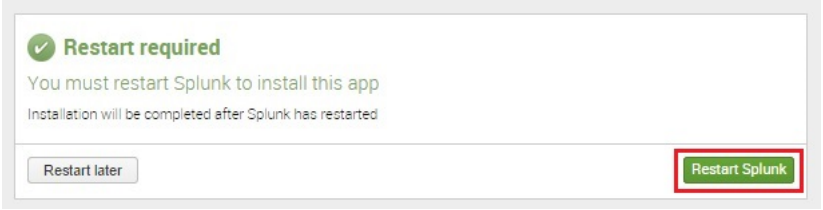
6. В окне **Upload an app** нажмите на кнопку **Upload**.



Кнопка **Upload**

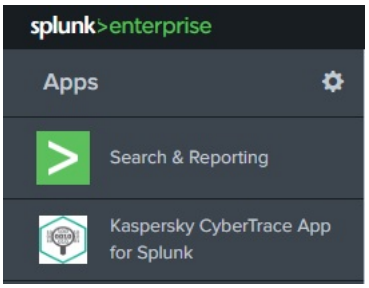
7. В окне **Restart required** нажмите кнопку **Restart Splunk**.

   В некоторых версиях Splunk этот шаг можно пропустить. Если в Splunk не отображается окно **Restart required**, пропустите этот шаг.



Кнопка **Restart Splunk**

8. Когда Splunk снова запустится, Forwarder App отобразится в списке установленных приложений. После установки Kaspersky Search Head App откроется страница **Apps** с информацией об успешной установке Kaspersky Search Head App. Kaspersky Search Head App появится в списке приложений на главной странице Splunk.



Kaspersky Search Head App для Splunk в списке приложений

Чтобы установить Forwarder App for Universal Forwarder, выполните следующие действия:

1. Распакуйте пакет Kaspersky-CyberTrace-App-for-Splunk_Universal-Forwarder.tar и поместите извлеченные файлы в папку Splunk_TA_Kaspersky-CyberTrace-App-for-Splunk-Universal-Forwarder в каталоге %SPLUNK_HOME%/etc/apps на используемом Forwarder (%SPLUNK_HOME% соответствует каталогу установки Splunk).

   Убедитесь, что в каталоге %SPLUNK_HOME%/etc/apps/Splunk_TA_Kaspersky-CyberTrace-App-for-Splunk-Universal-Forwarder существуют подкаталоги *default*, *metadata* и *static*, а также файл README.txt.

2. Скопируйте файл %SPLUNK_HOME%/etc/apps/SplunkUniversalForwarder/default/inputs.conf в %SPLUNK_HOME%/etc/system/local/inputs.conf и в двух позициях значения атрибута _TCP_ROUTING укажите имя активной группы с индексаторами.

   Если файл %SPLUNK_HOME%/etc/system/local/inputs.conf уже существует, выполните настройку вручную.

   По умолчанию эта группа имеет имя *default-autolb-group*. Фактическое имя групп индексаторов указано в файле %SPLUNK_HOME%/etc/system/local/outputs.conf. Настройки, заданные по умолчанию в файле inputs.conf, обеспечивают пересылку внутренних журналов Splunk Universal Forwarder во все источники, включая Kaspersky CyberTrace. Вышеперечисленные шаги позволяют пересылать журналы Splunk только в индексаторы.

   Пример содержимого файла %SPLUNK_HOME%/etc/system/local/inputs.conf:

   ```
   [monitor://%SPLUNK_HOME%/var/log/splunk/splunkd.log]
   _TCP_ROUTING = default-autolb-group
   index = _internal

   [monitor://%SPLUNK_HOME%/var/log/splunk/metrics.log]
   _TCP_ROUTING = default-autolb-group
   index = _internal
   ```

3. Перезапустите Splunk на Universal Forwarder:

   ```
   %SPLUNK_HOME%/bin/splunk restart
   ```

4. Перенесите все строки файла props.conf из каталога Forwarder %SPLUNK_HOME%/etc/apps/Splunk_TA_Kaspersky-CyberTrace-App-for-Splunk-Universal-Forwarder/default/props.conf в каталог Indexer %SPLUNK_HOME%/etc/system/local/props.conf.

   Если файл не существует, создайте новый файл.

Этот шаг необходим, поскольку Universal Forwarder не способен к парсингу событий, соответственно, настройки парсинга из props.conf не будут работать на Universal Forwarder. В этом случае парсинг событий будет выполняться непосредственно на индексаторе.

5. Перезапустите Splunk на индексаторе:

```
%SPLUNK_HOME%/bin/splunk restart
```

Шаг 2. Настройка Forwarder App и Search Head App (распределенное развертывание)

При использовании распределенной схемы развертывания необходимо настроить Forwarder App в соответствии со структурой используемой распределенной среды Splunk. Например, могут потребоваться следующие изменения настройки: изменение адреса Kaspersky CyberTrace Service, используемого приложениями, или добавление новых источников событий для Forwarder App. Для Search Head App может потребоваться настройка адресов электронной почты для оповещений.

Действия по настройке для Forwarder App и Search Head App

Для Forwarder App, возможно, потребуется выполнить следующие действия:

- Изменить адрес и порт для пересылки событий в Kaspersky CyberTrace Service. См. подраздел «Изменение адреса и порта для пересылки данных в Kaspersky CyberTrace Service» ниже.
- Настроить Forwarder App для отправки событий в один или несколько индексаторов. По умолчанию события, отправляемые из Forwarder App в Kaspersky CyberTrace Service, не регистрируются в индексах. См. подраздел «Настройка Forwarder App для отправки событий в индексы» ниже.
- Если используется несколько приложений Forwarder App, только одно приложение Forwarder App должно получать события от Kaspersky CyberTrace на порт `9998`. Для всех остальных Forwarder App это правило необходимо отключить путем указания значения `true` для параметра `disabled` для этого правила в конфигурационном файле Forwarder App. IP-адрес и порт Forwarder App, получающего события от Kaspersky CyberTrace, необходимо указать на странице **Параметры → Служба** в веб-интерфейсе Kaspersky CyberTrace.
- Добавить новые источники событий. См. подраздел «Добавление новых источников событий» ниже.

Для Search Head App может потребоваться выполнение следующих действий:

- Добавление адресов электронной почты в шаблоны оповещений.

После внесения изменений в конфигурационные файлы перезапустите Splunk.

Редактировать следует только те конфигурационные файлы Forwarder App и Search Head App, которые описаны в этом разделе. Редактирование других конфигурационных файлов может привести к непредсказуемому поведению.

Конфигурационные файлы (распределенное развертывание)

В следующей таблице приведены конфигурационные файлы, используемые Forwarder App и Search Head App в следующих вариантах распределенной схемы развертывания:

- Один индексатор, несколько форвардеров
- Несколько индексаторов, несколько форвардеров

Конфигурационные файлы Forwarder App и Search Head App

Приложение	Конфигурационный файл	Правила по умолчанию
Forwarder App	`\default\inputs.conf`	Получает данные из источников на порт `3000` и пересылает их в соответствии с параметрами, заданными в файле `outputs.conf`. Получает события от Kaspersky CyberTrace на порт `:9998`.
Forwarder App	`\default\outputs.conf`	Пересылает данные на `127.0.0.1:9999` (адрес Kaspersky CyberTrace Service).
Forwarder App	`\default\props.conf`	Парсинг данных, полученных на `:3000` и `:9998`. Описание правил парсинга данных по умолчанию приведено в подразделе «Правила парсинга данных по умолчанию» ниже.
Search Head App	`\default\savedsearches.conf`	Правила для шаблонов оповещений.

Правила парсинга данных по умолчанию

Способ парсинга входящих данных, применяемый в Splunk, задается в файле props.conf. По умолчанию в нем задаются следующие параметры:

- Определяется способ извлечения меток времени из входящих данных.
- Определяется разделитель (перенос строки) между событиями для входящих данных.

  Например, если входящие данные состоят из последовательности «`%data_1%\n\n%data_2%`», а перенос строки состоит из одного или нескольких символов `\n`, Splunk разбивает эту последовательность на два события (`%data_1%` и `%data_2%`).

Ниже приведены правила по умолчанию, используемые в Forwarder App для парсинга входящих данных.

```
TIME_PREFIX = ^
MAX_TIMESTAMP_LOOKAHEAD = 17
TIME_FORMAT = %b %d %H:%M:%S
LINE_BREAKER = ([\n]+)
SHOULD_LINEMERGE = false
```

В Universal Forwarder парсинг событий не предусмотрен. Настройки парсинга из props.conf не будут работать в Universal Forwarder. В этом случае парсинг событий будет выполняться непосредственно на индексаторе. См. Шаг 1. Установка приложений Forwarder App и Search Head App.

Изменение адреса и порта для пересылки данных в Kaspersky CyberTrace Service

По умолчанию в Forwarder App настроена пересылка данных в Kaspersky CyberTrace Service по адресу `127.0.0.1:9999`.

Чтобы изменить адрес и порт для пересылки данных в Kaspersky CyberTrace Service,

в конфигурационном файле `outputs.conf` в разделе `[tcpout:service9999]` укажите новые значения адреса и порта для Kaspersky CyberTrace Service в параметре `server`.

В следующем примере задается адрес Kaspersky CyberTrace Service `192.0.2.100:9999`.

```
[tcpout:service9999]
disabled=false
server = 192.0.2.100:9999
sendCookedData = false
```

Добавление новых источников событий

Чтобы добавить новые источники событий, отредактируйте файлы конфигурации приложения inputs.conf и props.conf.

Чтобы добавить новый источник событий, выполните следующие действия:

1. В файле inputs.conf укажите новый источник событий, использующий правило маршрутизации TCP `service9999`.

   Все данные из этого источника будут пересылаться в Kaspersky CyberTrace Service.

2. В файле props.conf укажите способ обработки данных из этого источника.

3. Перезапустите Splunk.

Убедитесь, что данные из нового источника событий успешно обрабатываются регулярными выражениям, используемыми Kaspersky CyberTrace.

Ниже приведен пример добавления адреса `:3001` в качестве источника событий; в примере задается, что данные с адреса `:3001` должны обрабатываться, как и другие входные данные в схеме интеграции по умолчанию (в этой схеме форвардер, индексатор и search head установлены на одном сервере).

```
# в inputs.conf
[tcp://:3001]
_TCP_ROUTING = service9999

# в props.conf
[source::tcp:3001]
TIME_PREFIX = ^
MAX_TIMESTAMP_LOOKAHEAD = 17
TIME_FORMAT = %b %d %H:%M:%S
LINE_BREAKER = ([\n]+)
SHOULD_LINEMERGE = false
```

Если для Splunk Forwarder уже настроено получение событий из разных источников событий и требуется отправлять события в Kaspersky CyberTrace Service, выполните действия в следующем порядке. Это возможно, если в поле `server` конфигурационного файла outputs.conf приложения Forwarder App заданы IP-адрес и порт, указанные в элементе `InputSettings > ConnectionString` конфигурационного файла Kaspersky CyberTrace Service.

Настройка пересылки событий в Kaspersky CyberTrace Service:

1. В файле outputs.conf, который используется для пересылки событий из Splunk (это может быть либо файл outputs.conf пользовательского приложения Splunk, либо файл `%SPLUNK_HOME%/etc/system/local/inputs.conf`), в поле `defaultGroup` добавьте запятую и строку `service9999`.

   В этом случае следует проверить логику пересылки событий и убедиться в том, что Splunk не отправляет события, поступающие из Kaspersky CyberTrace Service, обратно в Kaspersky CyberTrace Service.

Если файл конфигурации inputs.conf содержит параметр `_TCP_ROUTING` для тех источников событий, события из которых отправляются в Kaspersky CyberTrace Service, добавьте запятую и строку `service9999` в параметр `_TCP_ROUTING`.

2. Перезапустите Splunk.

При необходимости настройки ScannersCount в Kaspersky CyberTrace можно изменить в соответствии с архитектурой Splunk.

Настройка Forwarder App для отправки событий в индексы

По умолчанию события, отправляемые из Forwarder App в Kaspersky CyberTrace Service, не регистрируются в индексах. Это поведение можно изменить путем настройки Forwarder App.

Чтобы настроить в Forwarder App отправку событий в индекс main, выполните следующие действия:

1. Найдите Forwarder, который требуется настроить. Этот Forwarder обычно представляет собой хост с установленным Forwarder App. Необходимо настроить все Forwarder'ы, используемые в распределенной схеме интеграции.

2. На форвардере в файле `%SPLUNK_HOME%\etc\system\local\outputs.conf` найдите имя целевой группы, используемой для отправки событий в один или несколько индексаторов. Здесь `%SPLUNK_HOME%` соответствует каталогу установки Splunk.

   По умолчанию для этой группы задано имя «default-autolb-group»:

   ```
   [tcpout: default-autolb-group]
   ```

3. В файле `inputs.conf`, приложением Forwarder App, найдите раздел с правилом маршрутизации TCP `service9999`:

   ```
   _TCP_ROUTING = service9999
   ```

4. Добавьте в это правило имя целевой группы.

   Например, если имя целевой группы — «default-autolb-group», правило необходимо изменить следующим образом:

   ```
   _TCP_ROUTING=service9999, default-autolb-group
   ```

5. Перезапустите Splunk на форвардере.

Настройка шаблонов информационных сообщений

Дополнительная информация о настройке шаблонов предупреждений приведена в подразделе "Настройка шаблонов оповещений" раздела Шаг 2 (необязательный). Настройка Kaspersky CyberTrace App.

Шаг 3 (необязательный). Настройка скрипта поиска (распределенное развертывание)

Скрипт поиска используется для сопоставления отдельных URL, IP-адресов и хешей с потоками данных об угрозах Kaspersky Threat Data Feeds. Скрипт можно вызвать на вкладке **Indicators** в Kaspersky CyberTrace App Search Head.

Чтобы настроить скрипт поиска, выполните следующие действия:

1. В Kaspersky CyberTrace App перейдите на вкладку **Indicators lookup**.
2. Задайте строки подключения к Kaspersky CyberTrace:
   - В поле **Kaspersky CyberTrace address** укажите IP-адрес Kaspersky CyberTrace.
   - В поле **Kaspersky CyberTrace port** укажите порт, используемый Kaspersky CyberTrace.

Скрипт готов к использованию.

Шаг 4. Проверка работоспособности (Splunk, распределенная интеграция)

В случае распределенной интеграции Kaspersky CyberTrace со Splunk проверка работоспособности выполняется так же, как и проверка работоспособности для однокомпонентной схемы интеграции.

Интеграция с ArcSight ESM

В этой главе описывается порядок интеграции Kaspersky CyberTrace с ArcSight.

Общие сведения об интеграции (ArcSight)

В этой главе кратко описывается порядок интеграции Kaspersky CyberTrace с продуктами ArcSight.

О схемах интеграции

Возможны две схемы интеграции Kaspersky CyberTrace с ArcSight:

Порядок интеграции с ArcSight

Чтобы интегрировать Kaspersky CyberTrace с ArcSight, выполните следующие действия:

1. Перед установкой Kaspersky CyberTrace убедитесь, что выполнена установка ArcSight SmartConnector.
2. Убедитесь, что выполнена установка Kaspersky CyberTrace.
3. Импортируйте пакет Kaspersky_CyberTrace_Connector.arb package.
4. Установите ArcSight Forwarding Connector одним из двух способов:
   - Установите ArcSight Forwarding Connector с помощью интерфейса ArcSight.
   - Установите ArcSight Forwarding Connector с помощью консоли.
5. Настройте Kaspersky CyberTrace для взаимодействия с ArcSight.

6. Выполните проверку работоспособности.

> Перед изменением каких-либо настроек процесса сопоставления необходимо выполнить проверку работоспособности.

Предварительные условия (ArcSight)

Перед установкой Kaspersky CyberTrace необходимо установить ArcSight SmartConnector. В этом разделе описывается порядок установки ArcSight SmartConnector.

Установка ArcSight SmartConnector (Linux)

В этом разделе описывается порядок установки ArcSight SmartConnector.

Чтобы установить ArcSight SmartConnector, выполните следующие действия:

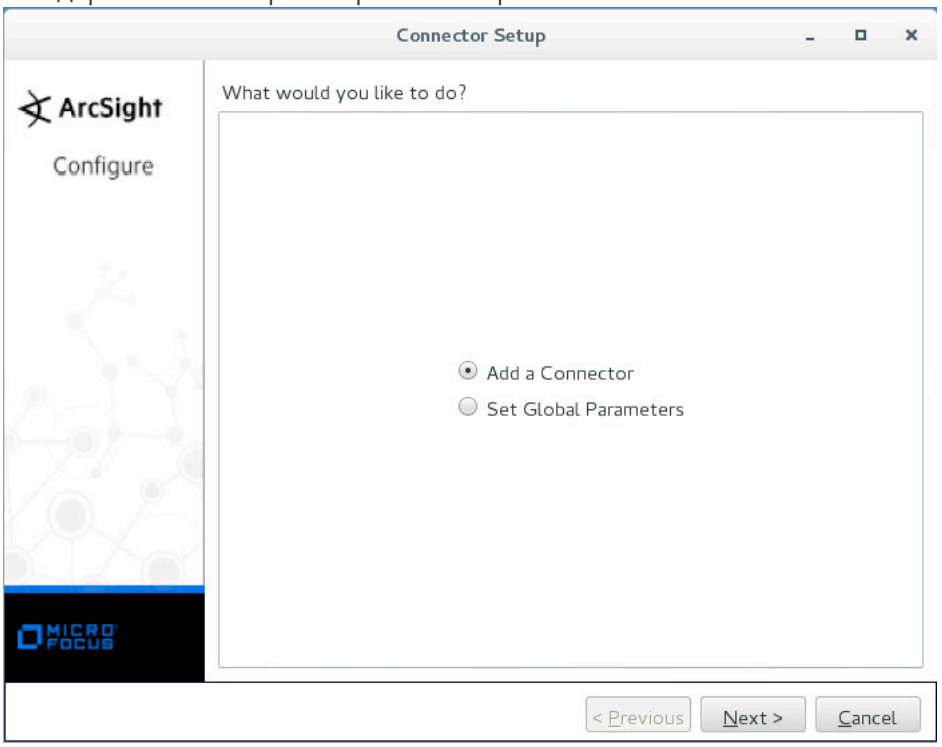
1. Запустите приложение установки ArcSight SmartConnector.

   Это приложение является компонентом HP ArcSight и не входит в состав Kaspersky CyberTrace.

2. Выберите каталог установки ArcSight SmartConnector (далее `%ARCSIGHT_HOME%`).

3. Отключите в установщике создание ссылок.

4. После распаковки содержимого бинарного файла выберите **Add a Connector**.



Добавление коннектора

Если это окно не отображается, настройте ArcSight SmartConnector вручную. Для этого выполните следующую команду:

```
%ARCSIGHT_HOME%/current/bin/runagentsetup.sh
```

5. В качестве типа коннектора выберите **Syslog Daemon**.

6. В форме **Enter the parameter details** укажите следующие данные:

- **Network Port** — порт, на который Kaspersky CyberTrace Service будет отправлять события обнаруженных киберугроз.

  Это тот же порт, который указан на странице **Параметры → Служба** веб-интерфейса Kaspersky CyberTrace (по умолчанию `9998`).

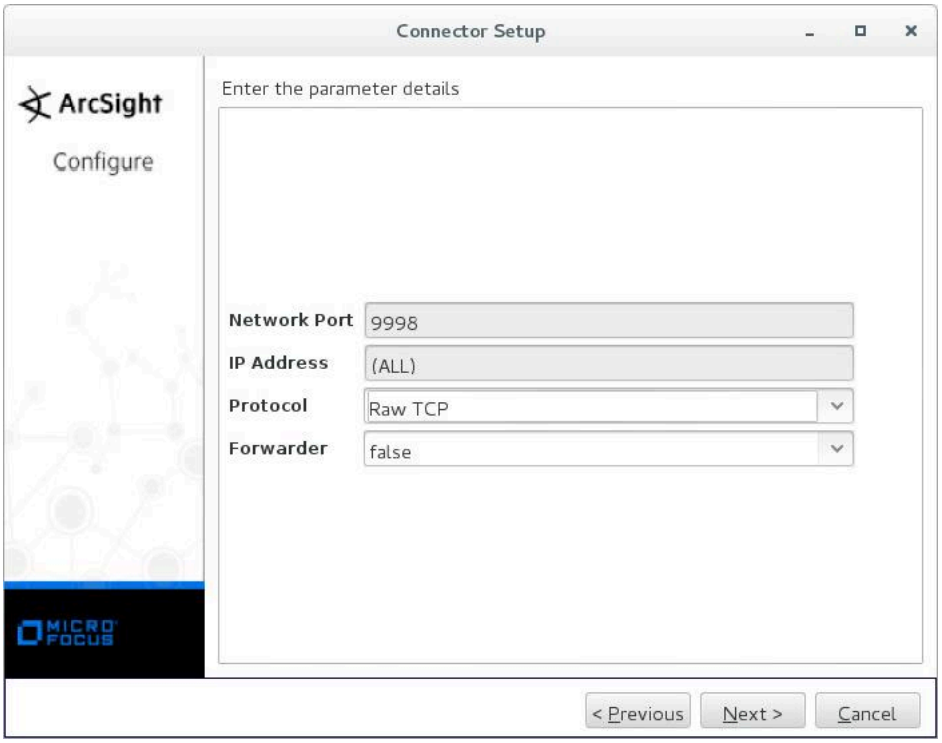
- **IP-адрес** — IP-адрес, на который Kaspersky CyberTrace Service будет отправлять события обнаруженных киберугроз.

  Это тот же IP-адрес, который указан на странице **Параметры → Служба** веб-интерфейса Kaspersky CyberTrace (по умолчанию `127.0.0.1`).

  > Если Arcsight SmartConnector должен принимать события со всех сетевых интерфейсов хоста, на котором он работает, можно указать `(ALL)`. (Обратите внимание, что указать `(ALL)` в конфигурационном файле Kaspersky CyberTrace Service невозможно).

- **Protocol** — укажите `Raw TCP`.

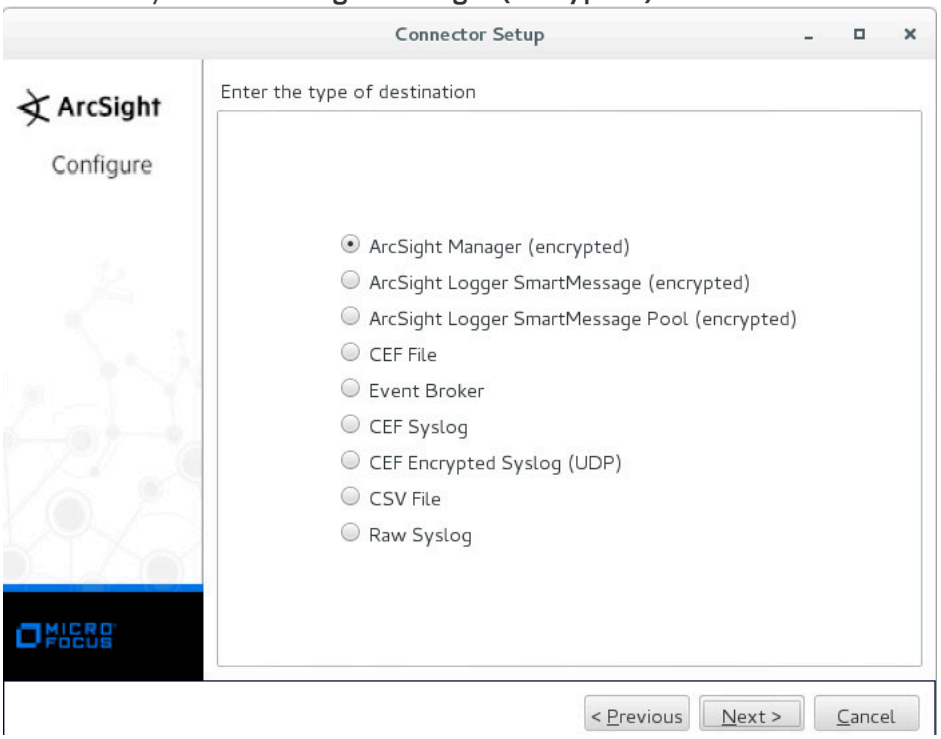
- **Forwarder** — укажите `false`.



Параметры отправки событий обнаруженных киберугроз

Нажмите на кнопку **Next**.

7. В качестве типа назначения укажите **ArcSight Manager (encrypted)**.



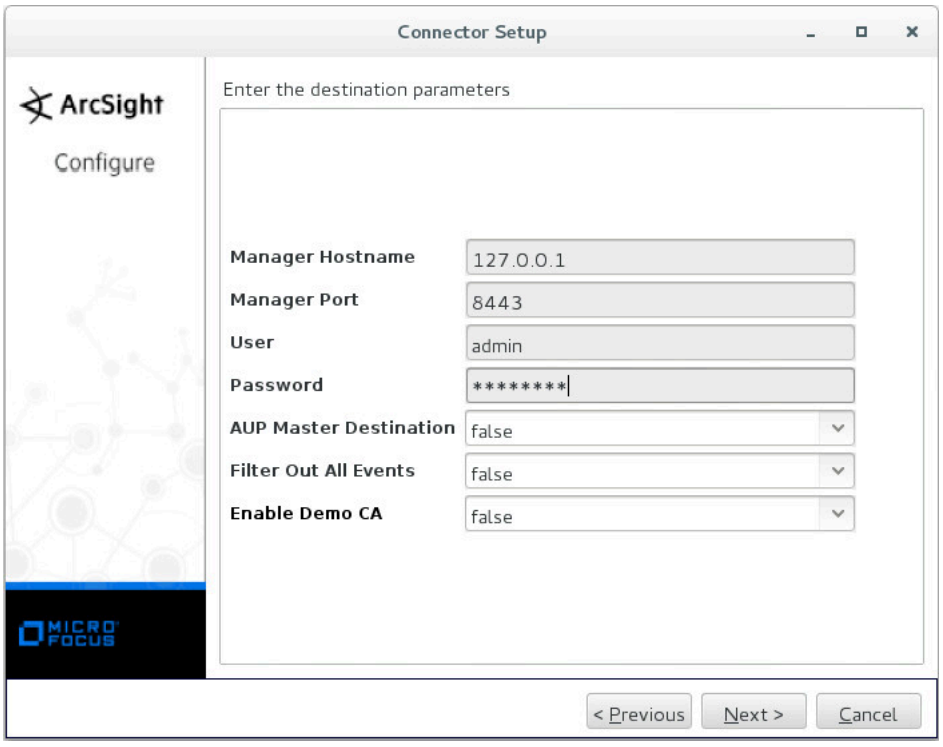
Тип назначения

Нажмите на кнопку **Next**.

8. Задайте другие параметры назначения:

- **Manager Hostname** — хост, на котором запущен ArcSight Manager.
- **Manager Port** — порт, на котором доступен ArcSight Manager.
  По умолчанию это порт 8443.
- **User** — имя пользователя ArcSight ESM, имеющего права на регистрацию коннектора.
- **Password** — пароль пользователя ArcSight ESM.
- **AUP Master Destination** — укажите `false`.

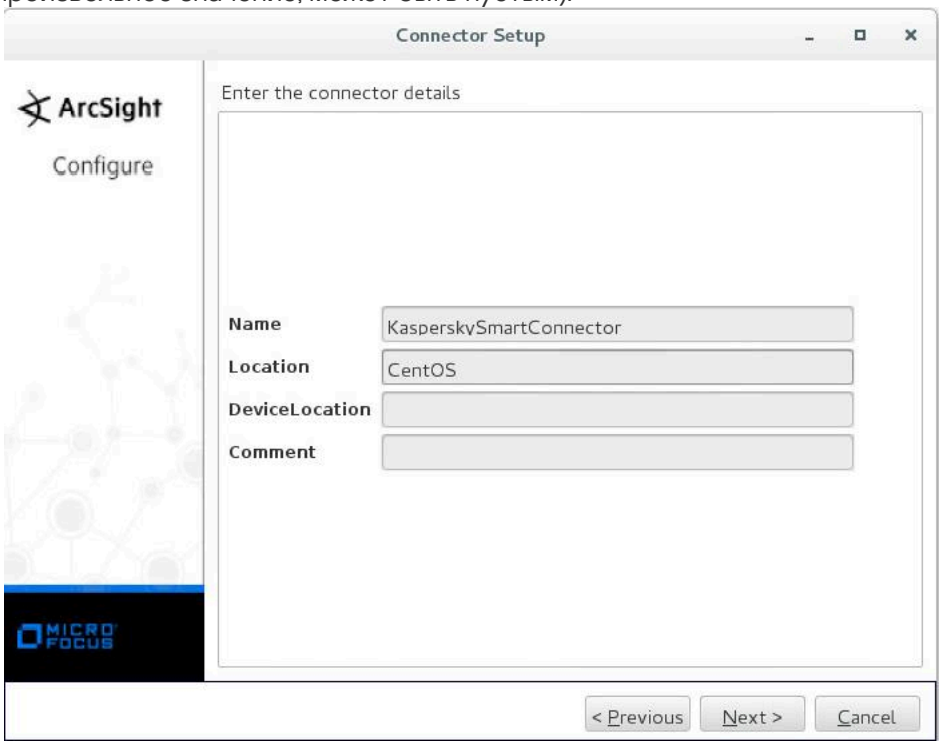
- **Filter Out All Events** — укажите `false`.
- **Enable Demo CA** — укажите `false`.



Параметры назначения

Нажмите на кнопку **Next**.

9. Укажите сведения о коннекторе: имя (можно указать произвольное значение), местоположение (можно указать произвольное значение), местоположение устройства, которое будет отправлять события в коннектор (можно указать произвольное значение, может быть пустым) и комментарий о коннекторе (можно указать произвольное значение, может быть пустым).

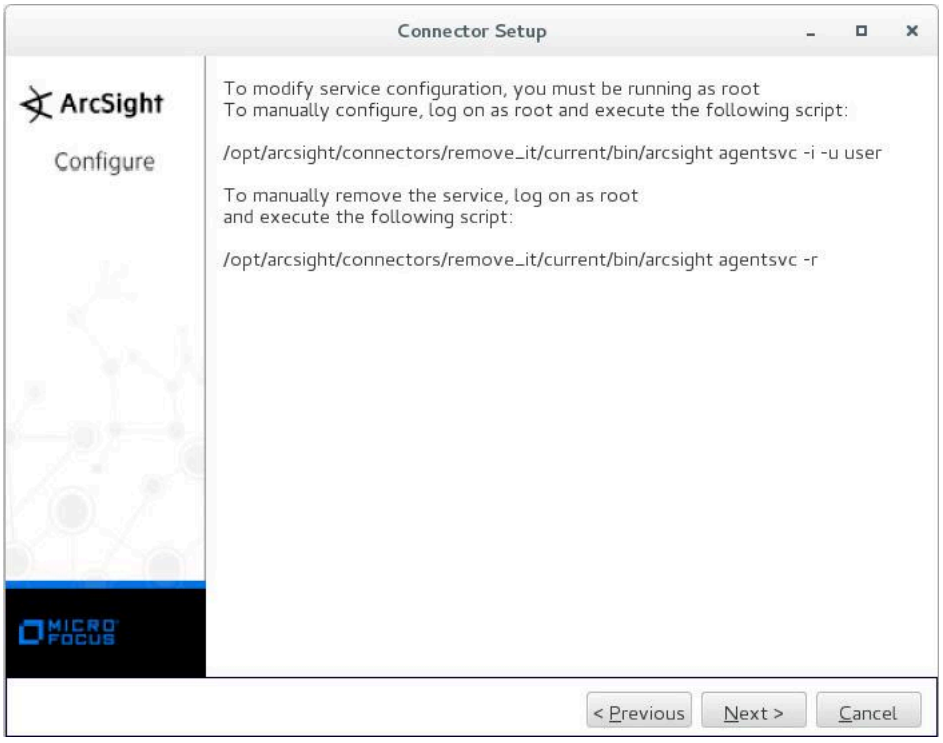


Подробные данные коннектора

Нажмите на кнопку **Next**.

10. Если параметры ArcSight Manager верны, примите импорт сертификата из места назначения.
11. Если сертификат импортирован успешно, установите службу ArcSight SmartConnector.

    - Если установка запущена без прав root, выводится предупреждение.



Предупреждение о правах пользователя

    Можно запустить мастер Connector Setup Wizard как root либо можно выполнить следующую команду как root:

    `%ARCSIGHT_HOME%/current/bin/arcsight agentsvc -i -u $username -sn $service_name`

    Параметры здесь имеют следующий смысл:

    - `$username` — имя пользователя операционной системы, который будет запускать службу.
    - `$service_name` — имя службы.

      Рекомендуется задать имя службы таким же, как имя коннектора.

    Сообщения о процессе установки будут добавлены в файл журнала `%ARCSIGHT_HOME%/current/logs/agent.log`.

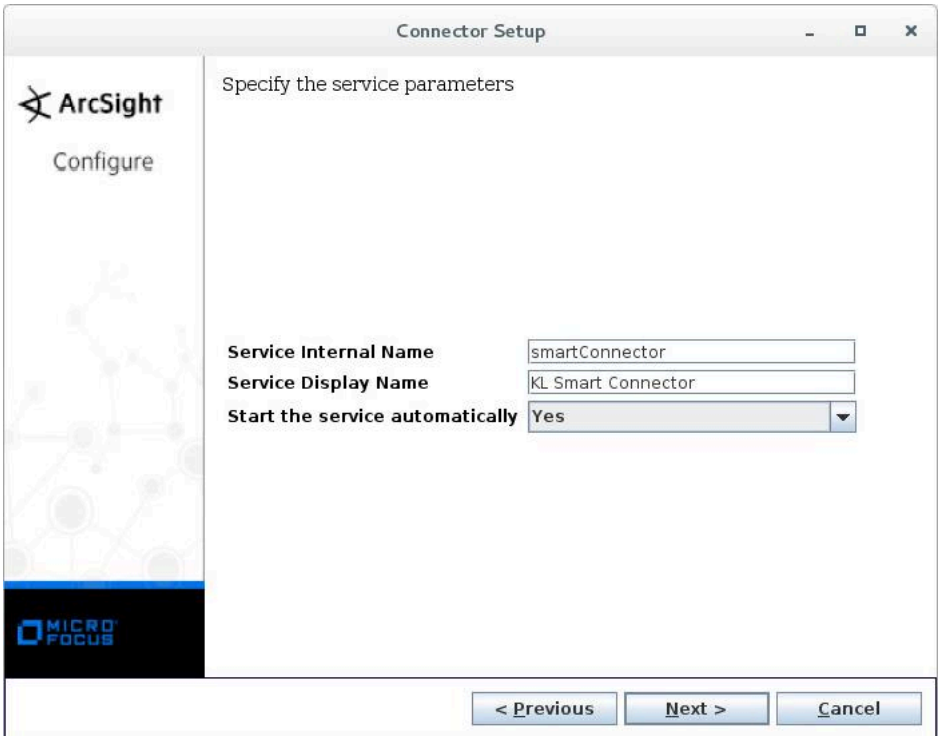
    Пропустите следующий шаг, описывающий указание параметров службы.

    - Если установка запускается от имени пользователя root, выберите **Install as a service**.

    Нажмите на кнопку **Next**.

12. Укажите параметры службы.

Рекомендуется задать имя службы таким же, как имя коннектора.



Указание параметров службы

Нажмите на кнопку **Next**.

13. Запустите ArcSight SmartConnector следующей командой:

    `/etc/init.d/arc_$service_name start`

    В этой команде `$service_name` соответствует имени службы.

После установки ArcSight SmartConnector можно установить Kaspersky CyberTrace Service и интегрировать его с ArcSight.

Установка ArcSight SmartConnector с помощью консоли (Linux)

Для установки ArcSight SmartConnector в ОС Linux вместо установщика с графическим интерфейсом пользователя можно воспользоваться консолью.

Чтобы установить ArcSight SmartConnector с помощью консоли, выполните следующие действия:

1. Запустите установщик ArcSight SmartConnector в консоли.
2. Прочтите раздел **Introduction** и нажмите клавишу **Enter**.
3. При появлении соответствующего запроса выберите **Choose Install Folder** и введите полный путь к каталогу, в который будет установлен ArcSight SmartConnector (`%ARCSIGHT_HOME%`).

   По умолчанию задан каталог `/root/ArcSightSmartConnectors`.
4. При появлении соответствующего запроса выберите **Choose Link Location** и укажите, требуется ли создавать ссылку на каталог установки.

   Рекомендуется выбрать вариант `Don't create links`.

5. Убедитесь, что в разделе **Pre-Installation Summary** указаны правильные значения настроек установки. Если значения правильные, нажмите клавишу **Enter**.

   После установки ArcSight SmartConnector в консоли выводится следующая информация:

   ```
   Installation Complete
   ---------------------
   The core components of the ArcSight SmartConnector have been successfully installed to:
   %ARCSIGHT_HOME%
   To finish the configuration of the SmartAgent, please go to the folder:
   %ARCSIGHT_HOME%/current/bin/
   and execute the script:
   ./runagentsetup.sh
   ```

6. Запустите скрипт `%ARCSIGHT_HOME%/current/bin/runagentsetup.sh`.

7. Запустите `Add a Connector`.

8. В качестве типа коннектора укажите `Syslog Daemon`.

9. Задайте следующие настройки коннектора:

   - **Network Port**

     Укажите порт, на который Kaspersky CyberTrace Service должен отправлять события. Это тот же порт, который указан на странице **Параметры → Служба** веб-интерфейса Kaspersky CyberTrace (по умолчанию `9998`).

   - **IP Address**

     Укажите IP-адрес, на который Kaspersky CyberTrace Service должен отправлять события. Это тот же порт, который указан на странице **Параметры → Служба** веб-интерфейса Kaspersky CyberTrace (по умолчанию `127.0.0.1`).

     > Укажите `ALL`, если хотите, чтобы Arcsight SmartConnector получал события со всех сетевых интерфейсов сервера, на котором он запущен. При этом параметр `ALL` недоступен в конфигурационном файле Kaspersky CyberTrace Service.

   - **Protocol**

     Укажите `Raw TCP`.

   - **Forwarder**

     Укажите `false`.

10. В качестве типа назначения укажите `ArcSight Manager (encrypted)`.

11. Укажите, требуется ли маскировать пароли.

    Рекомендуется указать `yes`.

12. Задайте следующие настройки подключения ArcSight Manager:

    - **Manager Hostname**

      Хост ArcSight Manager.

    - **Manager Port**

      Порт ArcSight Manager. По умолчанию `8443`.

    - **User**

      Имя пользователя, имеющего право регистрировать коннекторы в ArcSight.

    - **Password**

      Пароль указанного пользователя.

    - **AUP Master Destination**

      Укажите `False`.

    - **Filter Out All Events**

      Укажите `False`.

    - **Enable Demo CA**

      Укажите `False`.

13. Задайте следующие настройки коннектора:

    - **Имя**

      Можно указать произвольное значение.

    - **Расположение**

      Можно указать произвольное значение.

    - **DeviceLocation**

      Можно указать произвольное значение.

    - **Comment**

      Можно указать произвольное значение.

    После этого коннектор будет зарегистрирован.

14. Укажите следующее действие для импорта сертификата: `Import the certificate to connector from destination`.

15. Убедитесь, что отображаемые данные верны.

    Если отображаемые данные верны, введите `yes`.

16. Укажите способ установки коннектора: `Install as a service`.

17. Задайте настройки учетной записи:

    - **Service Internal Name**
    - **Service Display Name**
    - **Start the service automatically**

      Задает, должна ли служба запускаться при запуске системы. Рекомендуется указать `yes`.

18. Проверьте указанные данные. Если данные верны, нажмите клавишу **`Enter`**.

    Выполняется установка коннектора как службы.

19. Запустите коннектор следующей командой:

    `/etc/init.d/arc_$service_name start`

    В этой команде `$service_name` соответствует ранее указанному внутреннему имени службы.

После установки ArcSight SmartConnector можно установить Kaspersky CyberTrace и интегрировать его с ArcSight.

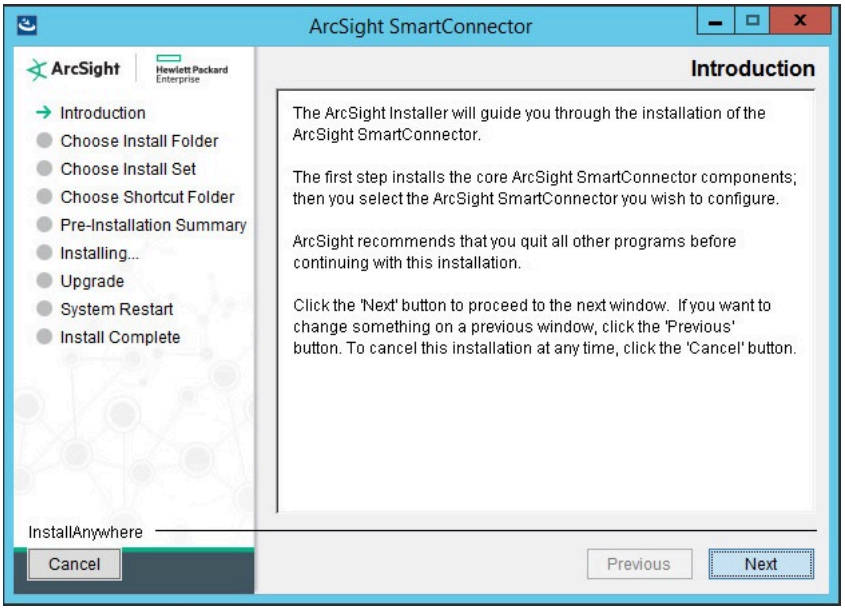
Установка ArcSight SmartConnector (Windows)

В этом разделе описывается порядок установки ArcSight SmartConnector в ОС Windows.

Чтобы установить ArcSight SmartConnector, выполните следующие действия:

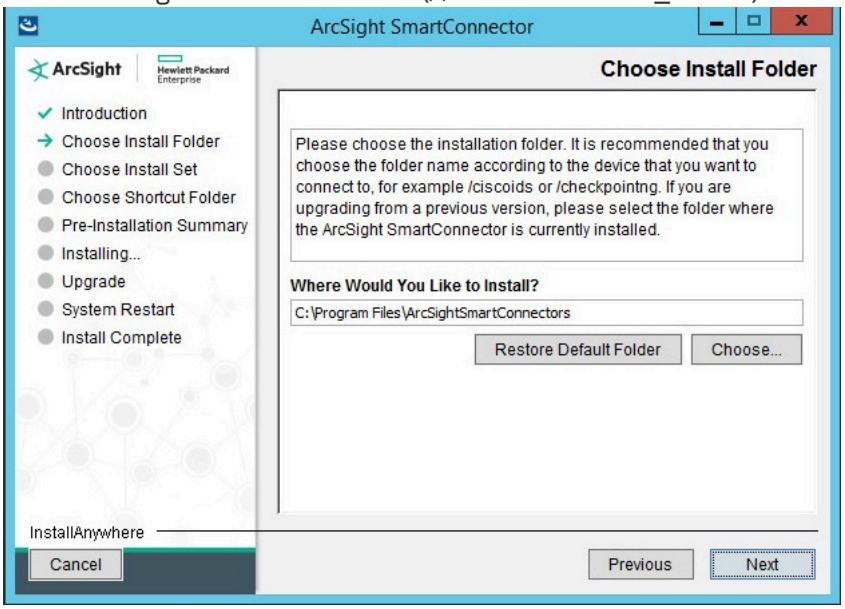
1. Запустите приложение установки ArcSight SmartConnector.

   Это приложение является компонентом HP ArcSight и не входит в состав Kaspersky CyberTrace.



Установка SmartConnector: введение

2. Выберите папку установки ArcSight SmartConnector (далее %ARCSIGHT_HOME%).

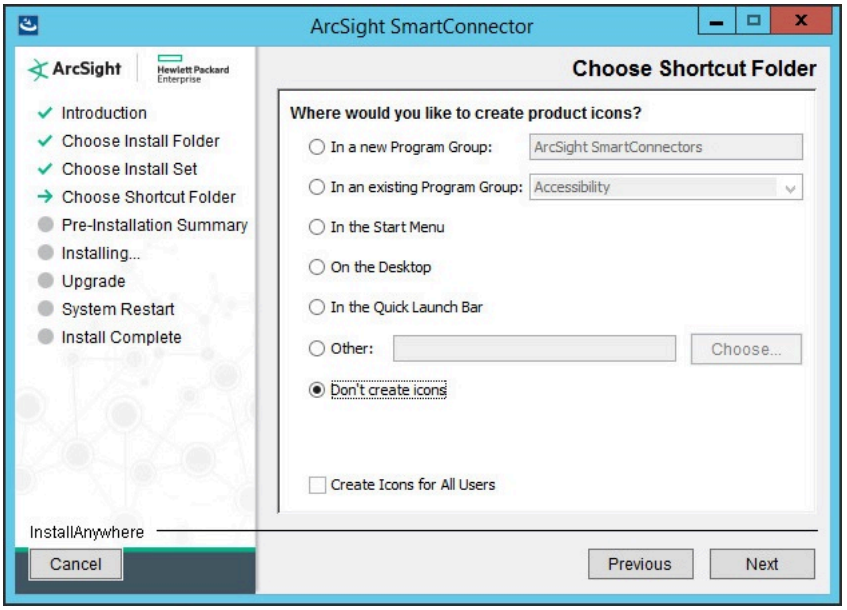


Выбор папки для установки

3. Выберите тип установки **Typical**.

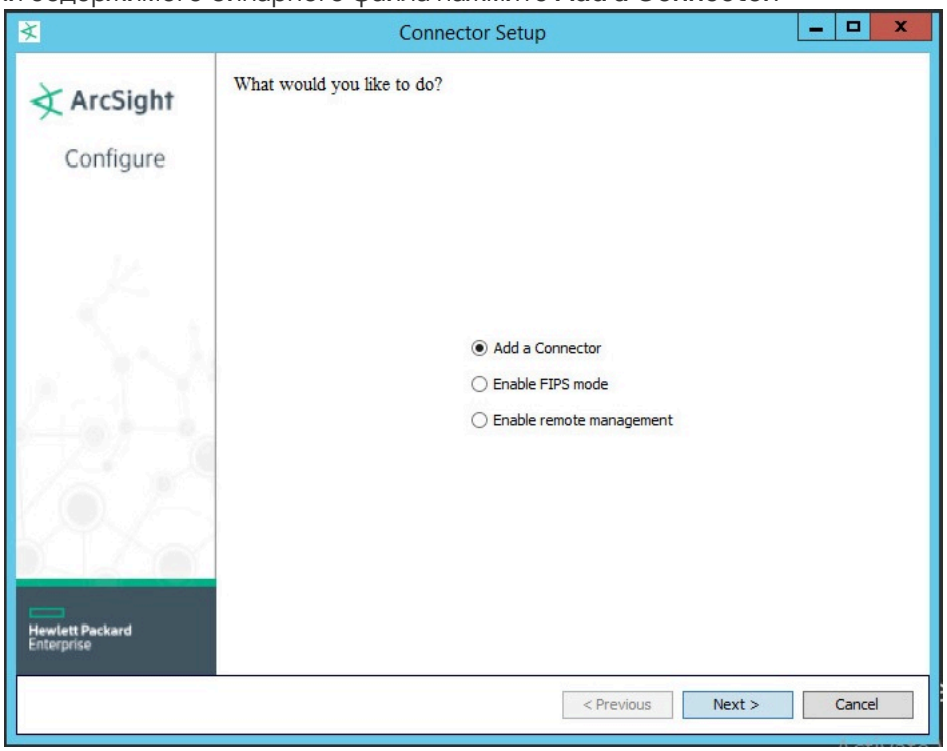
4. Выберите место, где будет создан ярлык для коннектора.

   Можно также отказаться от создания значков.



Выбор папки для ярлыка

5. После распаковки содержимого бинарного файла нажмите **Add a Connector**.

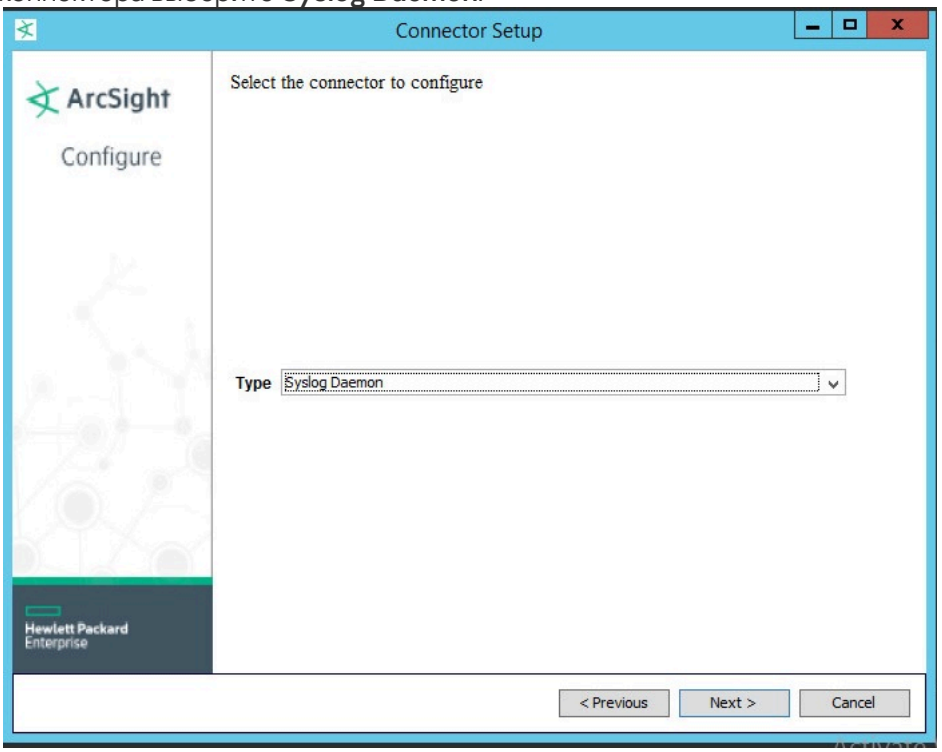


Добавление коннектора

Если это окно не отображается, настройте ArcSight SmartConnector вручную. Для этого выполните следующую команду:

```
%ARCSIGHT_HOME%\current\bin\runagentsetup.bat
```

6. В качестве типа коннектора выберите **Syslog Daemon**.



Выбор типа коннектора

Нажмите на кнопку **Next**.

7. В форме **Enter the parameter details** укажите следующие данные:

- **Network Port** — порт, на который Kaspersky CyberTrace Service будет отправлять оповещения об обнаружении индикаторов компрометации.

  Это тот же порт, который указан на странице **Параметры → Служба** веб-интерфейса Kaspersky CyberTrace (по умолчанию `9998`).

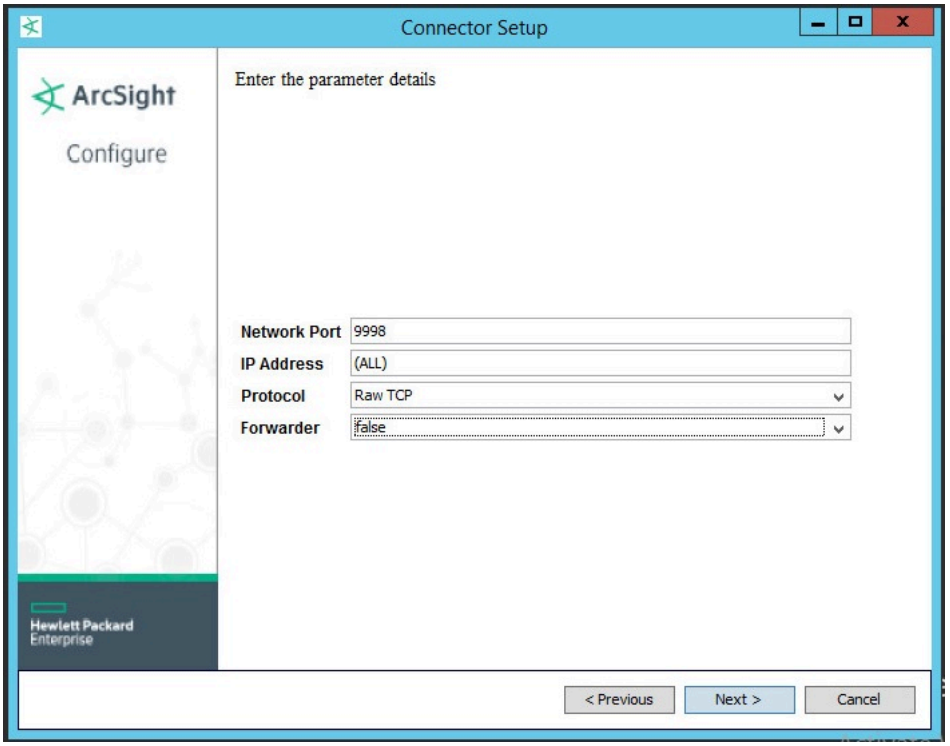
- **IP-адрес** — IP-адрес, на который Kaspersky CyberTrace Service будет отправлять оповещения об обнаружении индикаторов компрометации.

  Это тот же IP-адрес, который указан на странице **Параметры → Служба** веб-интерфейса Kaspersky CyberTrace (по умолчанию `127.0.0.1`).

  > Укажите `ALL`, если хотите, чтобы Arcsight SmartConnector получал события со всех сетевых интерфейсов сервера, на котором он запущен. При этом параметр `ALL` недоступен в конфигурационном файле Kaspersky CyberTrace Service.

- **Protocol** — укажите `Raw TCP`.

- **Forwarder** — укажите `false`.



Параметры отправки оповещений об обнаружении индикаторов компрометации

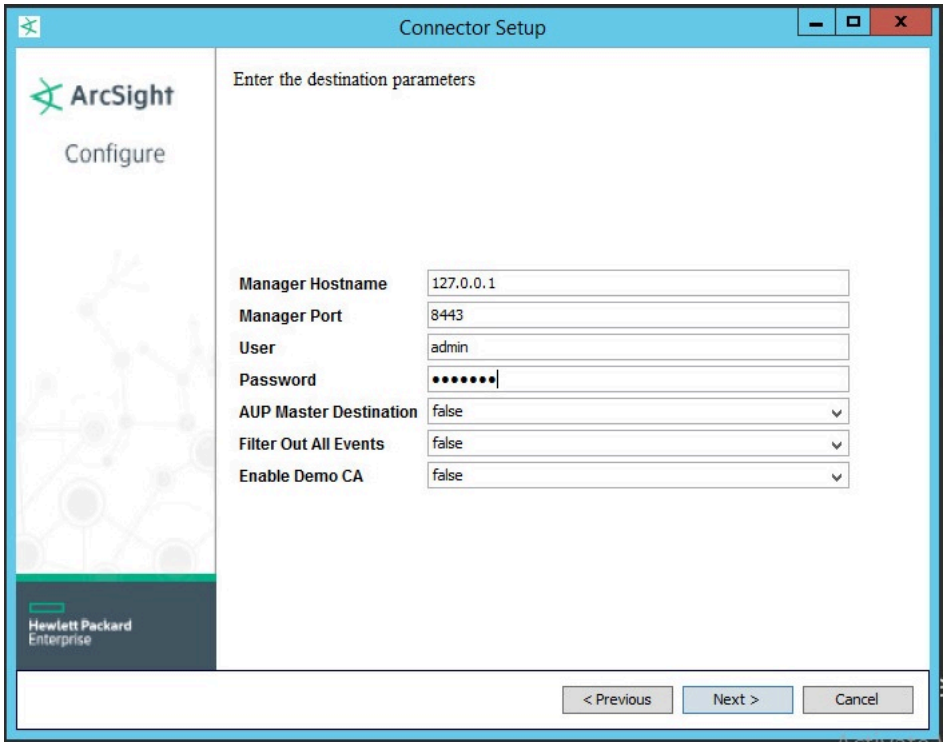
Нажмите на кнопку **Next**.

8. В качестве типа назначения укажите **ArcSight Manager (encrypted)**.

   Нажмите на кнопку **Next**.

9. Задайте другие параметры назначения:

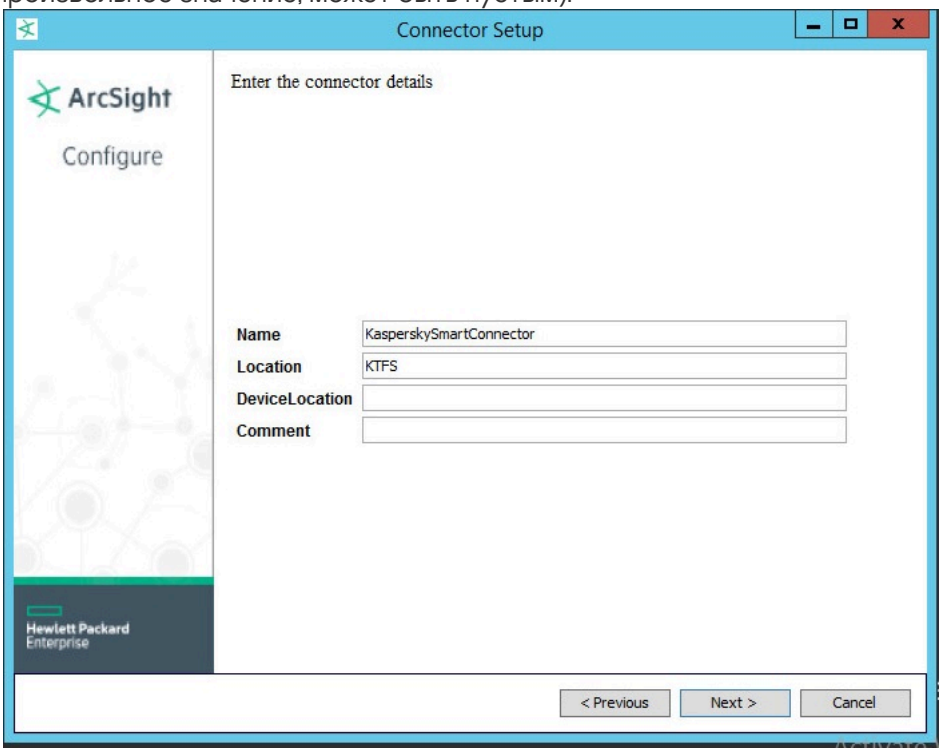
- **Manager Hostname** — хост, на котором запущен ArcSight Manager.
- **Manager Port** — порт, на котором доступен ArcSight Manager.
  По умолчанию это порт 8443.
- **User** — имя пользователя ArcSight ESM, имеющего права на регистрацию коннектора.
- **Password** — пароль пользователя ArcSight ESM.
- **AUP Master Destination** — укажите `false`.
- **Filter Out All Events** — укажите `false`.
- **Enable Demo CA** — укажите `false`.



Параметры назначения

Нажмите на кнопку **Next**.

10. Укажите сведения о коннекторе: имя (можно указать произвольное значение), местоположение (можно указать произвольное значение), местоположение устройства, которое будет отправлять события в коннектор (можно указать произвольное значение, может быть пустым) и комментарий о коннекторе (можно указать произвольное значение, может быть пустым).

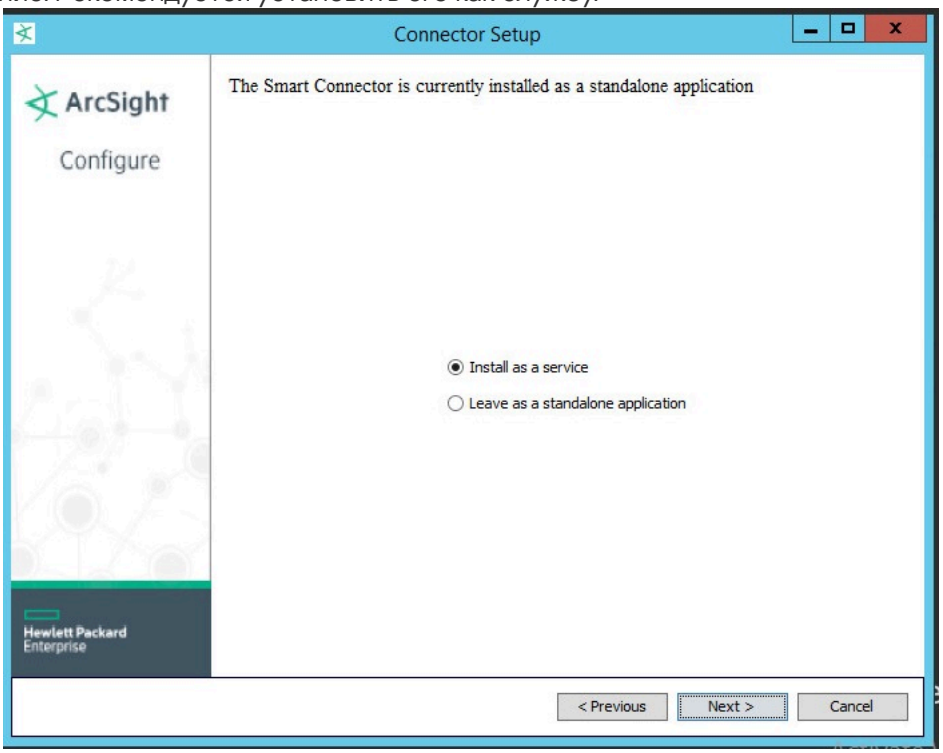


Подробные данные коннектора

Нажмите на кнопку **Next**.

11. Если параметры ArcSight Manager правильные, примите импорт сертификата из места назначения.

12. Если сертификат импортирован успешно, предлагается установить ArcSight SmartConnector как службу или как приложение. Рекомендуется установить его как службу.

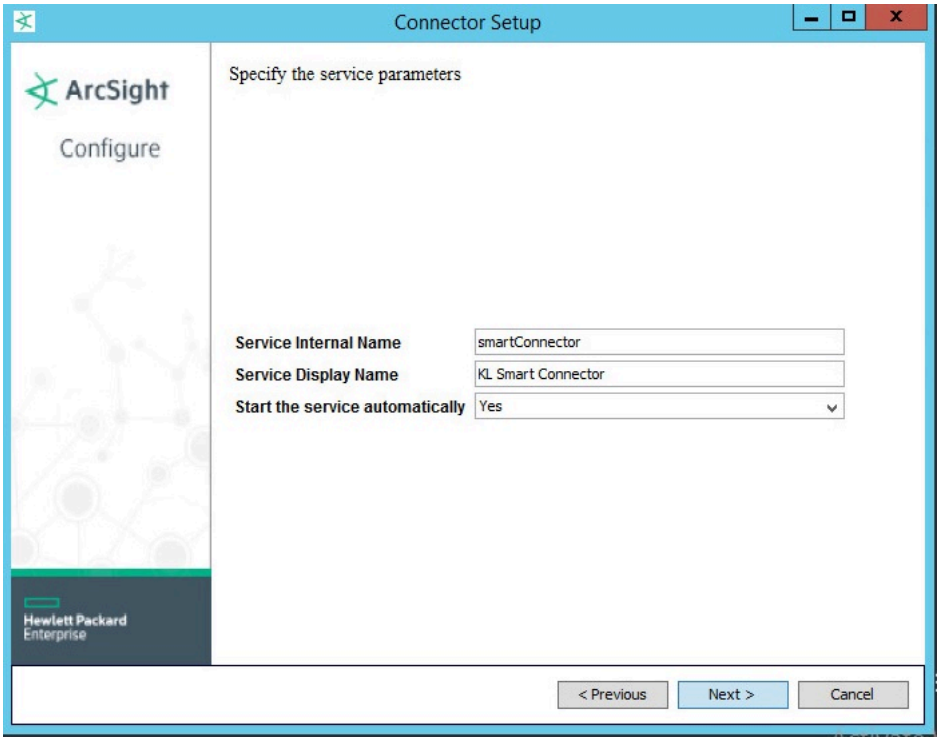


Выбор режима установки

Нажмите на кнопку **Next**.

13. Укажите параметры службы.

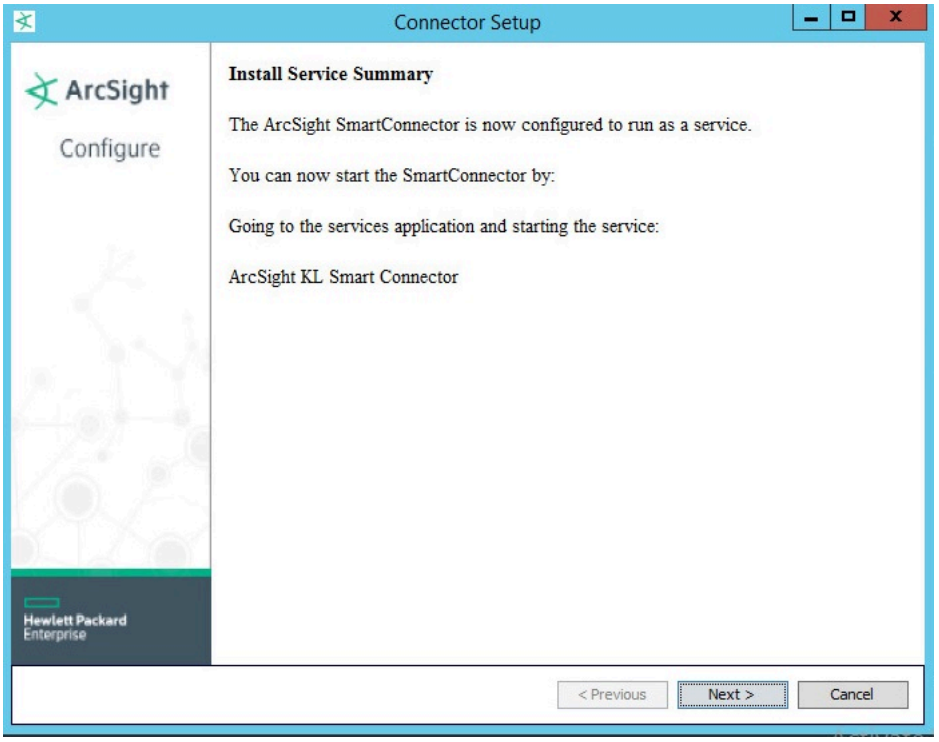
    Рекомендуется задать имя службы таким же, как имя коннектора.



Указание параметров службы

    Нажмите на кнопку **Next**.

    Отображается сводка операции.



Установка SmartConnector: сводка операции

14. В конфигурационном файле `%ARCSIGHT_HOME%/current/user/agent/agent.properties` задайте значение `30000` для параметра `agents[0].tcppeerclosedchecktimeout`.

15. Убедитесь, что служба с именем `ArcSight %ServiceDisplayName%` запущена (`%ServiceDisplayName%` — это имя, заданное в поле **Service Display Name** на предыдущем шаге).

    Для этого откройте Диспетчер задач Windows и проверьте статус службы. Статус должен быть `Работает`. С помощью Диспетчер задач Windows, можно остановить или запустить службу.

Стандартная интеграция (ArcSight)

В этом разделе описывается порядок интеграции Kaspersky CyberTrace и ArcSight по различным схемам интеграции.

Схемы интеграции (ArcSight)

В этом разделе описаны возможные схемы интеграции продуктов ArcSight и Kaspersky CyberTrace.

О компонентах стандартной схемы интеграции

В схемах интеграции для ArcSight используются следующие компоненты:

- ArcSight ESM

  Эта SIEM-система используется в этой интеграции.

  Этот компонент работает только в Linux.

- Forwarding Connector

  Этот компонент ArcSight отправляет события ArcSight в Kaspersky CyberTrace Service.

  Этот компонент работает только в Linux.

- Kaspersky CyberTrace Service

  Эта служба сопоставляет события ArcSight с потоками данных об угрозах Kaspersky Threat Data Feeds.

- SmartConnector

  Этот компонент ArcSight отправляет события, генерируемые Kaspersky CyberTrace Service, в ArcSight.

- Средства контроля безопасности

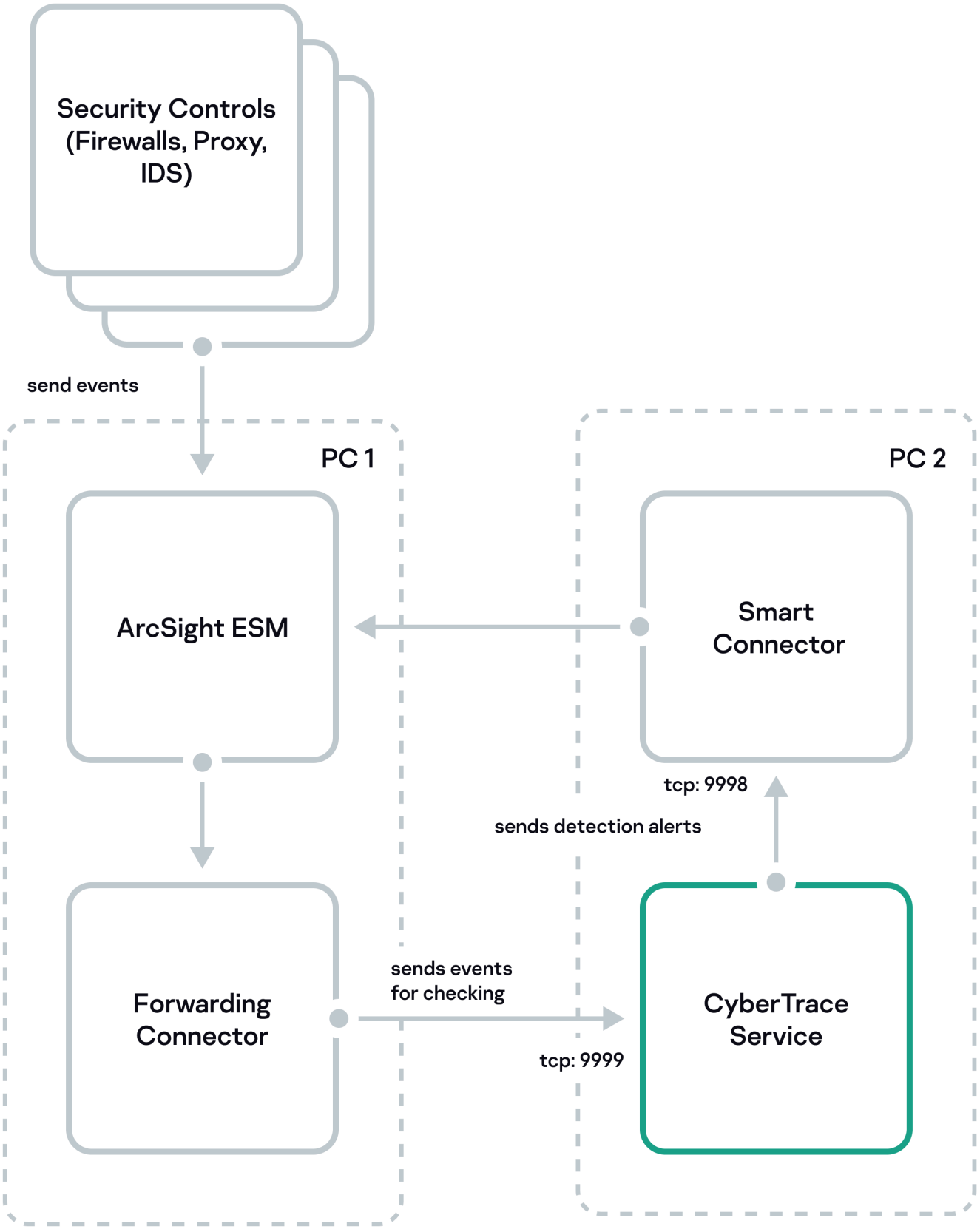
  Это источники событий для ArcSight, такие как межсетевые экраны, прокси-серверы, системы обнаружения вторжений и другие сетевые устройства. Средства контроля безопасности могут отправлять события в ArcSight любым способом, поддерживаемым ArcSight.

ArcSight ESM, ArcSight Forwarding Connector, ArcSight SmartConnector и Kaspersky CyberTrace Service можно устанавливать на различные серверы согласно указанным ниже схемам. Чтобы снизить влияние на производительность, рекомендуется устанавливать ArcSight ESM на отдельный сервер без установленных ArcSight Forwarding Connector, ArcSight SmartConnector и Kaspersky CyberTrace Service.

На рисунках в следующих разделах показаны некоторые возможные схемы интеграции.

Установка на двух серверах (рекомендуемый вариант интеграции)

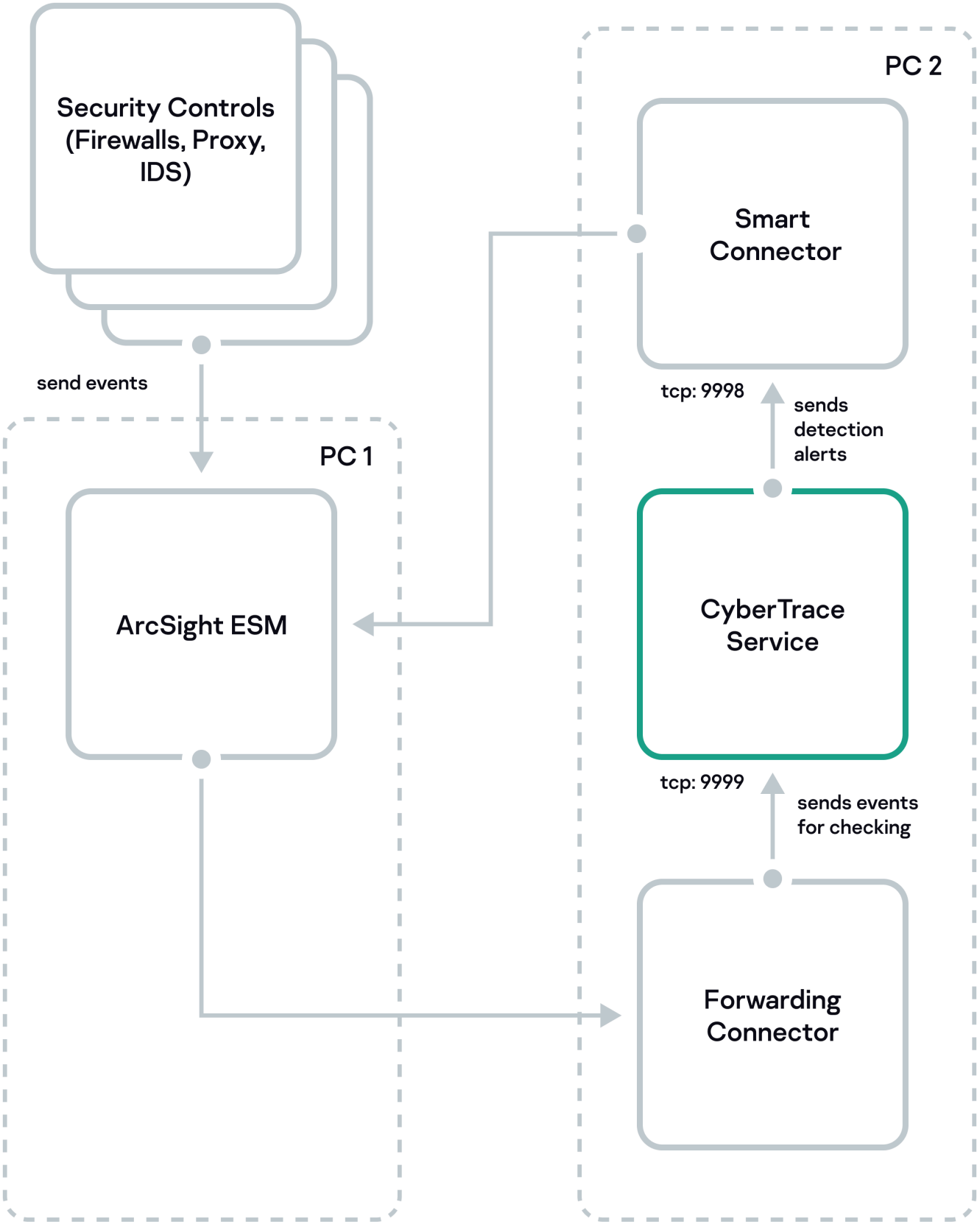
На рисунке ниже показаны ArcSight ESM и Forwarding Connector, установленные на одном сервере, а также Kaspersky CyberTrace Service и SmartConnector, установленные на другом сервере.



Установка на двух серверах (рекомендуемый вариант интеграции)

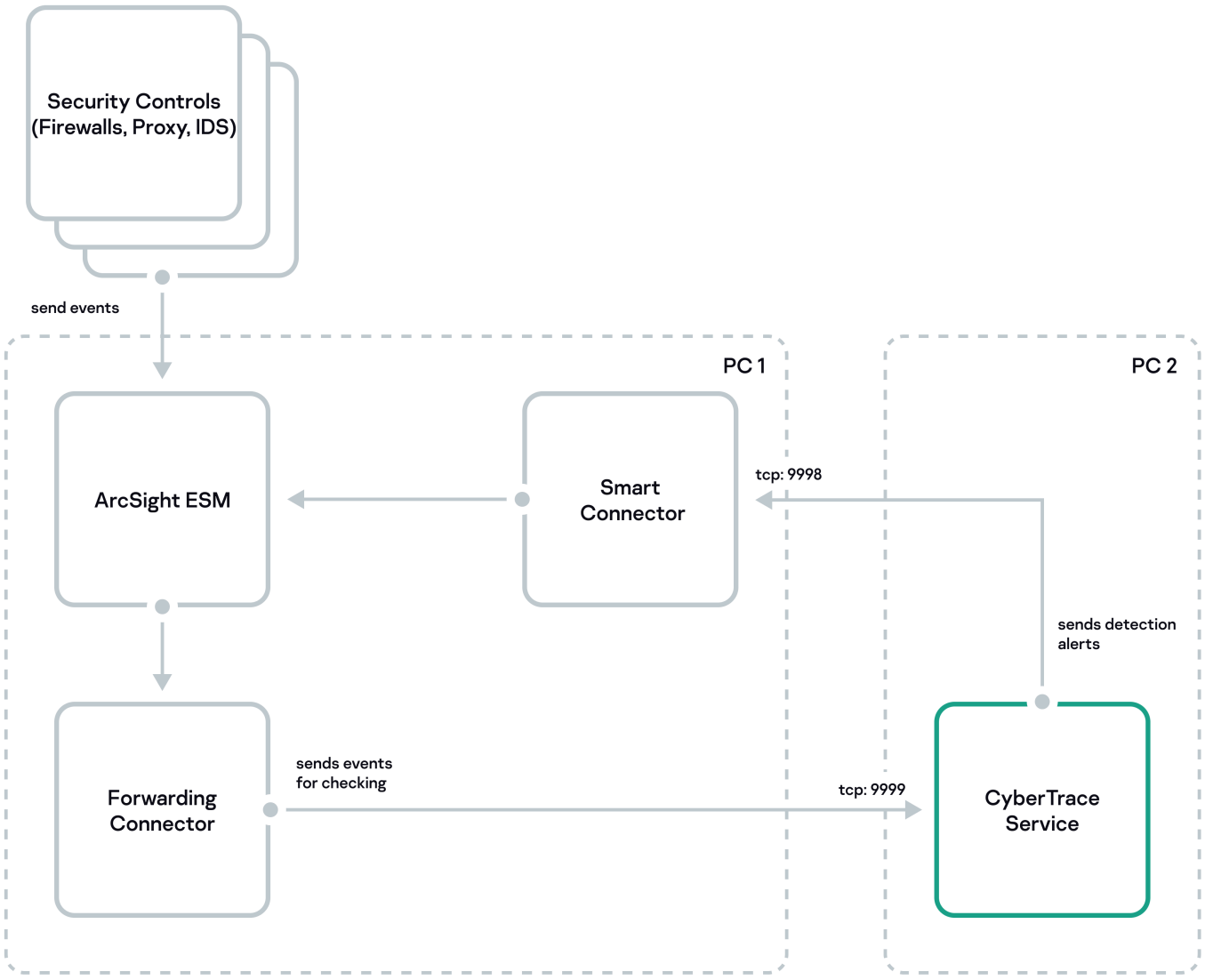
Установка на двух серверах (второй рекомендуемый вариант интеграции)

На рисунке ниже показан ArcSight ESM, установленный на одном сервере, а также Forwarding Connector, Kaspersky CyberTrace Service и SmartConnector, установленные на другом сервере. Эта схема применима, только если Kaspersky CyberTrace работает под управлением Linux, в противном случае используйте другую схему установки.



Установка на двух серверах (третий рекомендуемый вариант интеграции)

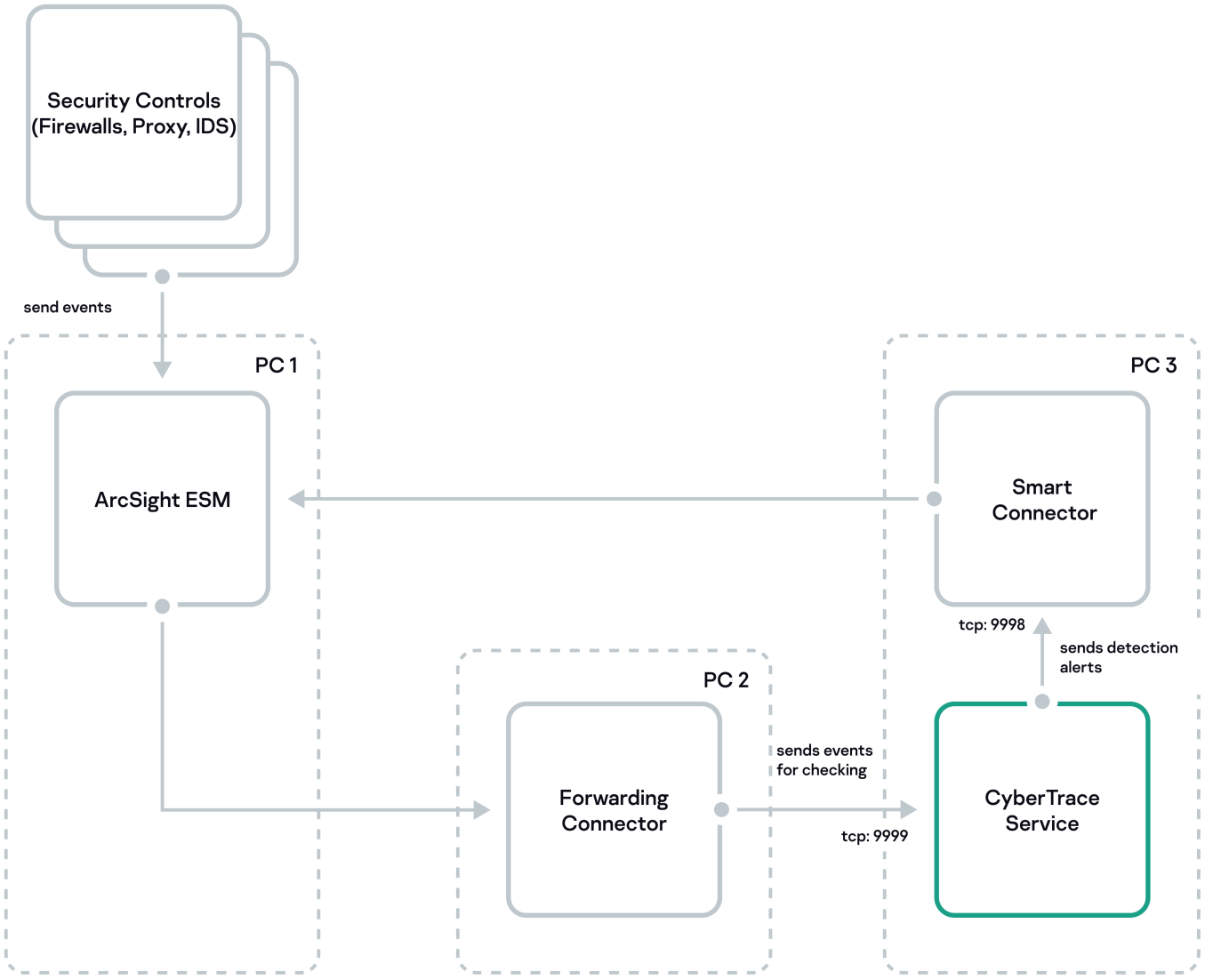
На рисунке ниже показан Kaspersky CyberTrace Service, установленный на одном сервере, а также SmartConnector, ArcSight ESM и Forwarding Connector, установленные на другом сервере.



Установка на двух серверах (третий рекомендуемый вариант интеграции)

Установка на трех серверах

На рисунке ниже показан ArcSight ESM, установленный на одном сервере, Forwarding Connector, установленный на другом сервере, а также Kaspersky CyberTrace Service и SmartConnector, установленные на третьем сервере.



Установка на трех серверах

Шаг 1. Импорт пакета ARB

В этом разделе описывается порядок импорта пакета ARB в ArcSight.

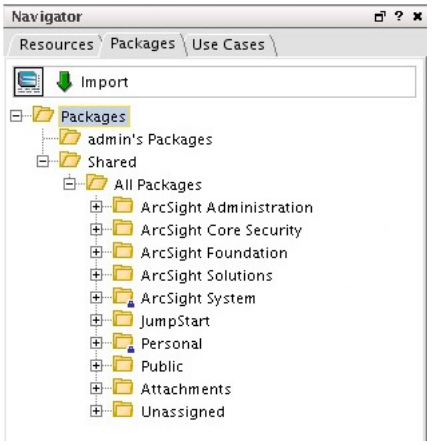
Пакет ARB содержит объекты (активные каналы, информационные панели, наборы полей, отчеты, правила, фильтры, пользователи), которые необходимы для интеграции службы с ArcSight. При импорте этого файла эти объекты создаются в ArcSight.

Чтобы импортировать пакет ARB, выполните следующие действия:

1. Запустите ArcSight Console.

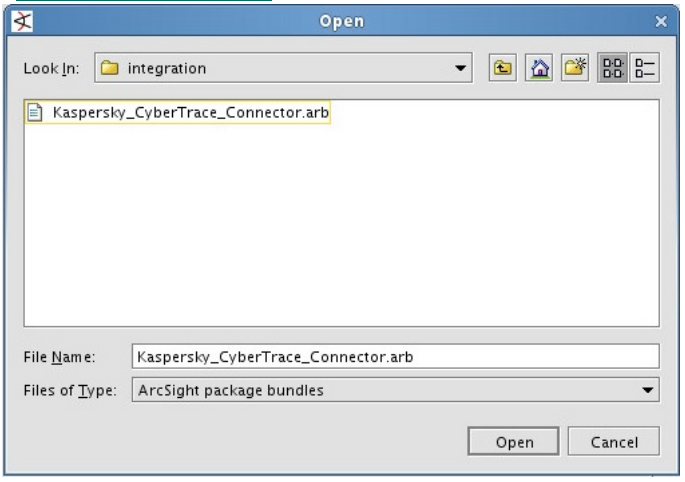
2. На панели **Navigator** (в виде дерева) выберите вкладку **Packages**.

3. Нажмите на кнопку **Import**.



Пакеты ArcSight

4. В окне **Open** выберите файл Kaspersky_CyberTrace_Connector.arb file, расположенный в каталоге `/integration/arcsight/` комплекта поставки.



Выбор файла ARB

Процесс импорта будет выполнен.



Импорт ARB завершен

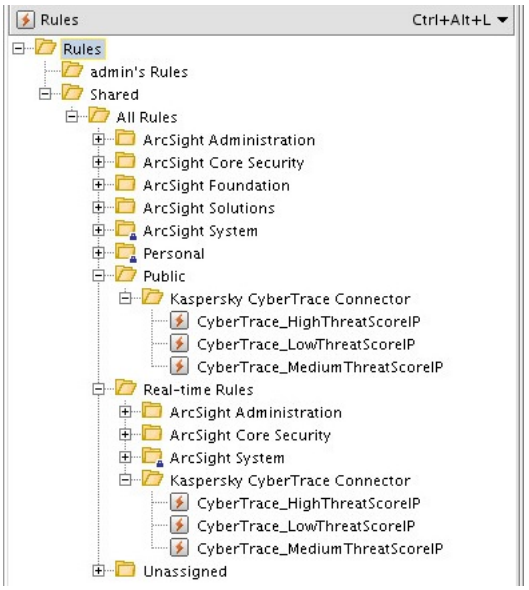
После того, как все объекты из файла ARB будут импортированы в ArcSight, все импортированные правила становятся правилами реального времени, то есть они применяются в режиме реального времени.

Для просмотра и настройки списка правил реального времени выполните следующие действия:

1. На виде дерева выберите вкладку **Resources**.

2. Откройте раскрывающийся список **Active Channels** и выберите **Rules**.

3. В дереве выберите **Rules** → **Shared** → **All Rules** → **Real-time Rules**.



Правила реального времени

4. Разверните элемент **Real-time Rules** и удалите из него ненужные вложенные элементы.

После импорта пакета ARB в ArcSight создаются новые объекты.

- Если в дереве выбран элемент **Active Channels**, по пути **Active Channels** → **Shared** → **All Active Channels** → **Public** → **Kaspersky CyberTrace Connector** расположены следующие объекты:

Object	Описание	Состояние по умолчанию
CyberTrace alerts	Отображает служебные оповещения из Kaspersky CyberTrace в режиме реального времени.	Включено
CyberTrace all matches	Отображает оповещения об обнаружении индикаторов компрометации из Kaspersky CyberTrace в режиме реального времени.	Включено
CyberTrace hash matches	Отображает оповещения об обнаружении хешей из Kaspersky CyberTrace в режиме реального времени.	Выключено
CyberTrace URL matches	Отображает оповещения об обнаружении URL из Kaspersky CyberTrace в режиме реального времени.	Выключено
CyberTrace IP matches	Отображает оповещения об обнаружении IP-адресов из Kaspersky CyberTrace в режиме реального времени.	Выключено

- Если в дереве выбран элемент **Dashboards**, по пути **Dashboards** → **Shared** → **All Dashboards** → **Public** → **Kaspersky CyberTrace Connector** расположены следующие объекты:

Object	Описание	Состояние по умолчанию
CyberTrace Detection map	Отображаются все устройства, которые отправляли события, содержащие вредоносные URL, IP-адреса или хеши. Отображает все потоки данных об угрозах, которые были задействованы в процессе обнаружения киберугроз.	Выключено
CyberTrace match statistics	Статистика обнаруженных киберугроз: сколько объектов той или иной категории было обнаружено.	Включено
CyberTrace TOP 10 matched indicators	Топ-10 обнаруженных индикаторов.	Выключено

Информационные панели `CyberTrace detection map` и `CyberTrace Top 10 matched indicators` по умолчанию выключены, чтобы не перегружать ArcSight. Если эти информационные панели необходимы, их можно включить.

- Если в дереве выбран элемент **Field Sets**, по пути **Field Sets → Shared → All Field Sets → Public → Kaspersky CyberTrace Connector** расположены следующие объекты:

Object	Описание	Состояние по умолчанию
CyberTrace alerts	Отображаются поля служебных оповещений из Kaspersky CyberTrace.	Статическое
CyberTrace all matches	Отображаются поля оповещения об обнаружении индикаторов компрометации из Kaspersky CyberTrace.	Статическое
CyberTrace matched hashes	Отображаются поля оповещений об обнаружении хешей из Kaspersky CyberTrace.	Статическое
CyberTrace matched URLs	Отображаются поля оповещений об обнаружении URL из Kaspersky CyberTrace.	Статическое
CyberTrace matched IPs	Отображаются поля оповещений об обнаружении IP-адресов из Kaspersky CyberTrace.	Статическое

- Если в дереве выбран элемент **Reports**, по пути **Reports → Shared → All Reports → Public → Kaspersky CyberTrace Connector** расположены следующие объекты:

Object	Описание	Состояние по умолчанию
CyberTrace all matches	Отчет, содержащий оповещения об обнаружении индикаторов компрометации из Kaspersky CyberTrace.	Статическое

- Если в дереве выбран элемент **Rules**, по пути **Rules → Shared → All Rules → Public → Kaspersky CyberTrace Connector** расположены следующие объекты:

Object	Описание	Состояние по умолчанию
CyberTrace_HighThreatScoreIP	Правило присвоения высокого уровня важности и хранения высокоприоритетных оповещений об обнаружении IP-адресов из Kaspersky CyberTrace.	Включено
CyberTrace_MediumThreatScoreIP	Правило присвоения среднего уровня важности и хранения среднеприоритетных оповещений об обнаружении IP-адресов из Kaspersky CyberTrace.	Включено
CyberTrace_LowThreatScoreIP	Правило присвоения низкого уровня важности и хранения низкоприоритетных оповещений об обнаружении IP-адресов из Kaspersky CyberTrace.	Включено

- Если в дереве выбран элемент **Filters**, по пути **Filters → Shared → All Filters → Public → Kaspersky CyberTrace Connector** расположены следующие объекты:

Object	Описание	Состояние по умолчанию
CyberTrace all matches	Фильтр для выбора оповещений об обнаружении индикаторов компрометации, отправленных из Kaspersky CyberTrace.	Статическое
CyberTrace forwarding events	Фильтр для пересылки в Kaspersky CyberTrace событий, содержащих URL, IP-адреса или хеши.	Статическое
CyberTrace matched hashes	Фильтр для выбора оповещений об обнаружении хешей, отправленных из Kaspersky CyberTrace.	Статическое
CyberTrace matched URLs	Фильтр для выбора оповещений об обнаружении URL, отправленных из Kaspersky CyberTrace.	Статическое
CyberTrace matched IPs	Фильтр для выбора оповещений об обнаружении IP-адресов, отправленных из Kaspersky CyberTrace.	Статическое

- Если в дереве выбран элемент **Users**, по пути **Users → Shared → Custom User Groups → Kaspersky CyberTrace Connector** расположены следующие объекты:

Object	Описание	Состояние по умолчанию
FwdCyberTrace	Учетная запись, используемая для настройки пересылки событий ArcSight.	Статическое

После завершения импорта проверьте, создан ли пользователь `FwdCyberTrace`. Чтобы убедиться в этом, перейдите в раздел **Users** → **Shared** → **Custom User Groups** → **Kaspersky CyberTrace Connector** в консоли ArcSight. Если пользователя `FwdCyberTrace` нет, создайте его вручную.

Шаг 2. Установка ArcSight Forwarding Connector

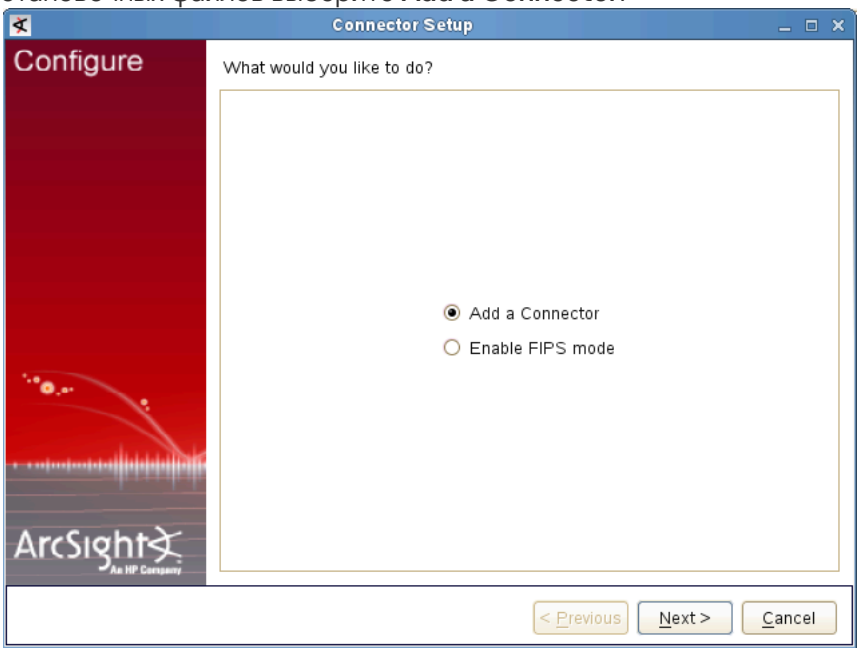
В этом разделе описывается порядок установки ArcSight Forwarding Connector.

ArcSight Forwarding Connector является компонентом HP ArcSight и не входит в состав Kaspersky CyberTrace. Это приложение можно получить одним из следующих способов:

- Обратитесь в службу поддержки HP для получения ArcSight Forwarding Connector.
- Для получения ArcSight Forwarding Connector обращайтесь по адресу intelligence@kaspersky.com.

Чтобы установить ArcSight Forwarding Connector, выполните следующие действия:

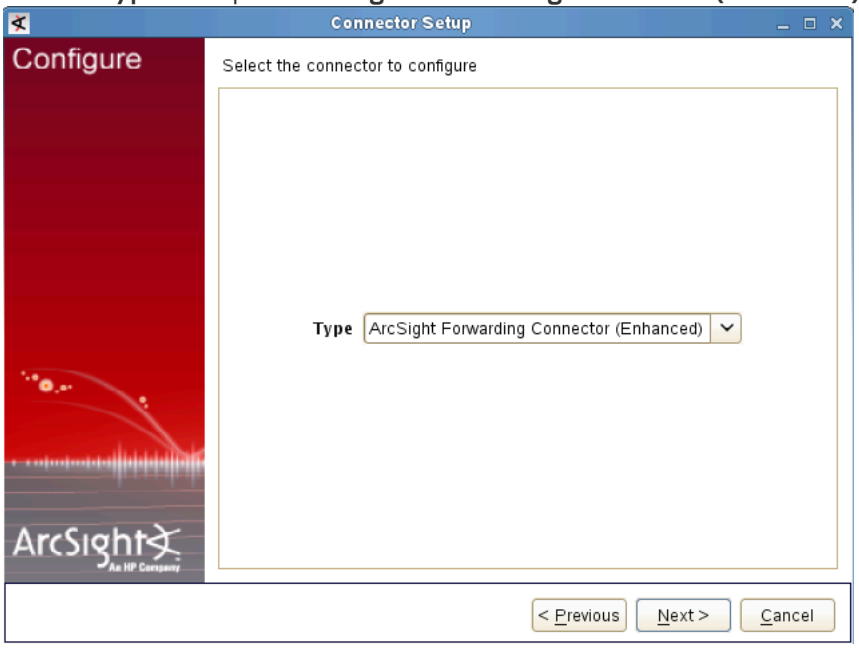
1. Запустите приложение установки ArcSight Forwarding Connector.
2. Выберите каталог установки ArcSight Forwarding Connector (далее `%ConnectorInstallDir%`).
3. После распаковки установочных файлов выберите **Add a Connector**.



Добавление коннектора

Нажмите на кнопку **Next**.

4. В раскрывающемся списке **Type** выберите **ArcSight Forwarding Connector (Enhanced)**.



Выбор типа коннектора

Нажмите на кнопку **Next**.

5. Укажите следующие параметры подключения ArcSight Source Manager:

- **Host Name**

  Хост ArcSight Source Manager.

- **Port**

  Порт ArcSight Source Manager (по умолчанию `8443`).

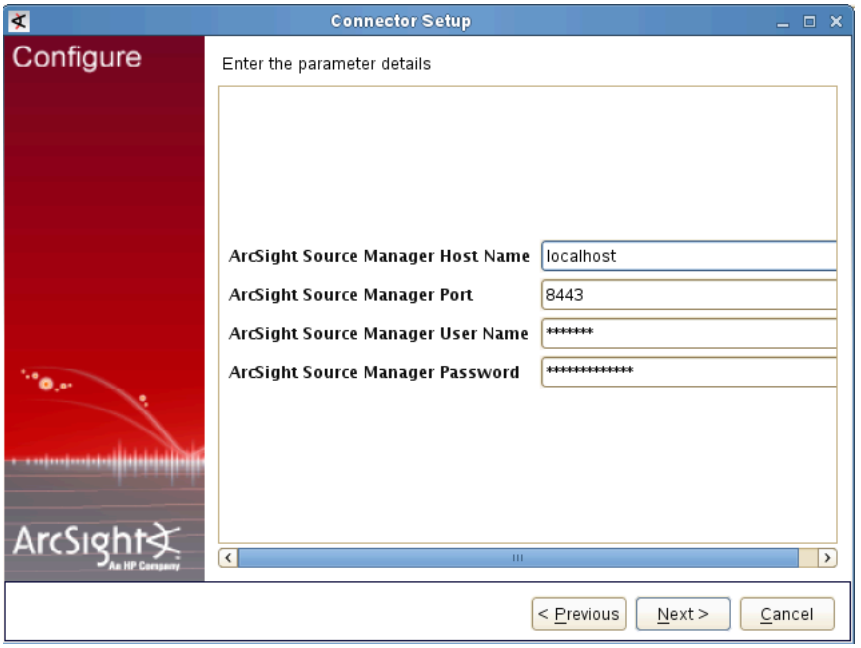
- **User Name**

  Имя пользователя учетной записи, которую должен использовать ArcSight Forwarding Connector (по умолчанию `FwdCyberTrace`).

  Вместо `FwdCyberTrace` можно указать другого пользователя. Для этого укажите собственного пользователя ArcSight в настройках ArcSight Forwarding Connector.

- **Password**

  Пароль от учетной записи, которую должен использовать ArcSight Forwarding Connector (по умолчанию `KasperskyLab!`).

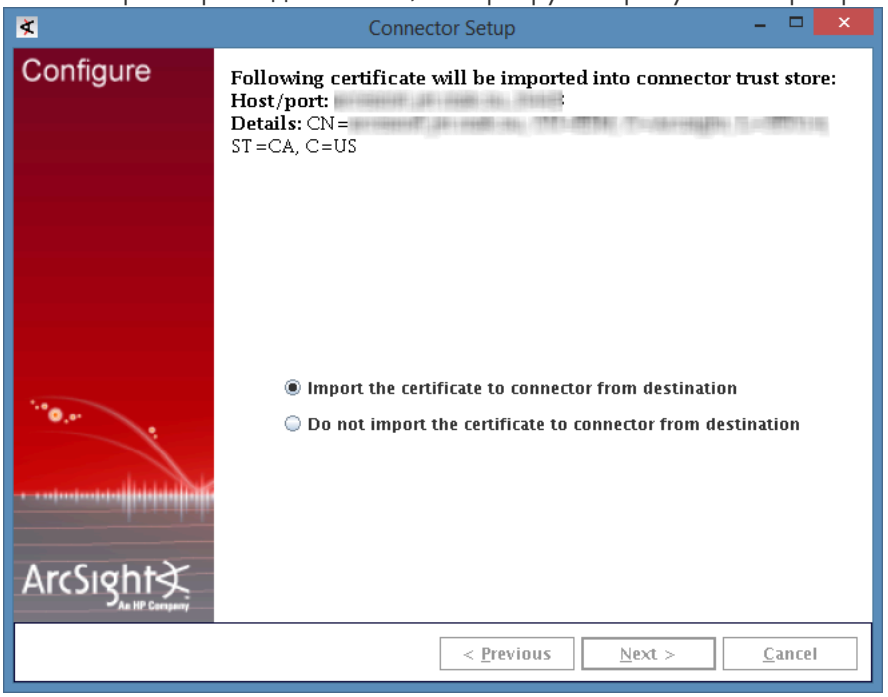


Параметры ArcSight Source Manager

Если возникает ошибка аутентификации (неверное имя пользователя или пароль), рекомендуется проверить, присутствует ли пользователь `FwdCyberTrace` в ArcSight Console. Если нет, создайте его вручную.

Нажмите на кнопку **Next**.

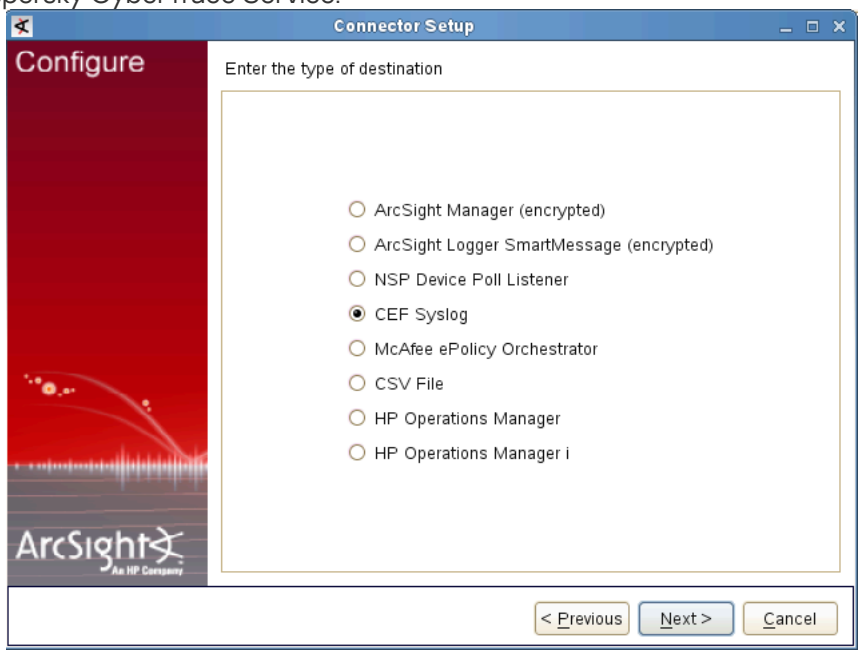
6. Если указаны правильные параметры подключения, импортируйте требуемый сертификат.



Импорт сертификата

Нажмите на кнопку **Next**.

7. Укажите **CEF Syslog** в качестве формата событий, который будет использоваться для событий, отправляемых в Kaspersky CyberTrace Service.

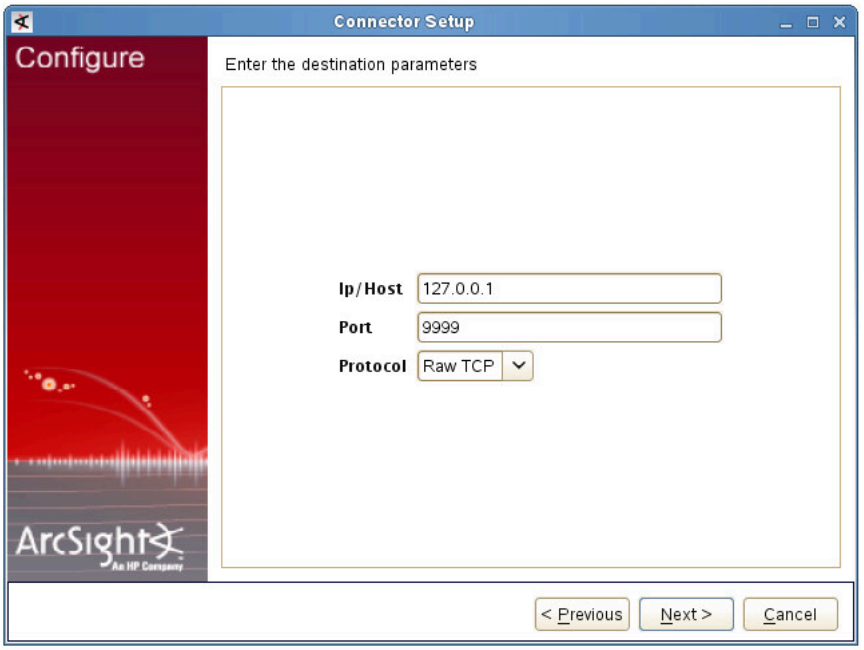


Настройка формата события

Нажмите на кнопку **Next**.

8. Укажите IP-адрес (или хост) и порт, который Kaspersky CyberTrace Service будет прослушивать для получения событий. В качестве протокола укажите **Raw TCP**.

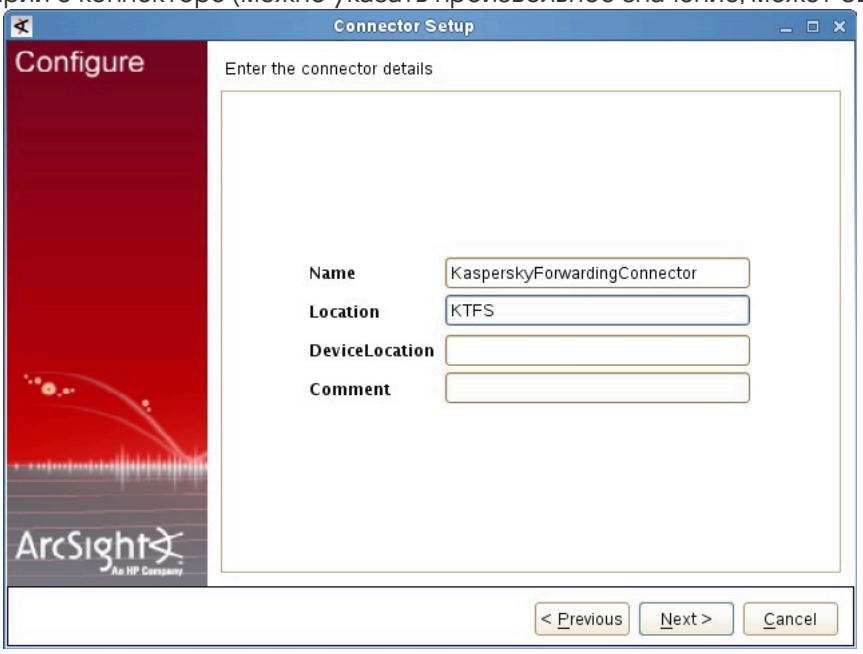
   IP-адрес и порт совпадают с указанными на странице **Параметры → Служба** веб-интерфейса Kaspersky CyberTrace. По умолчанию в качестве IP-адреса и порта для получения событий от ArcSight используется `127.0.0.1:9999`.



Настройка назначения события

Нажмите на кнопку **Next**.

9. Укажите сведения о новом объекте ArcSight Forwarding Connector: имя (можно указать произвольное значение), местоположение (можно указать произвольное значение), местоположение устройства, которое будет отправлять события в коннектор (можно указать произвольное значение, может быть пустым) и комментарий о коннекторе (можно указать произвольное значение, может быть пустым).

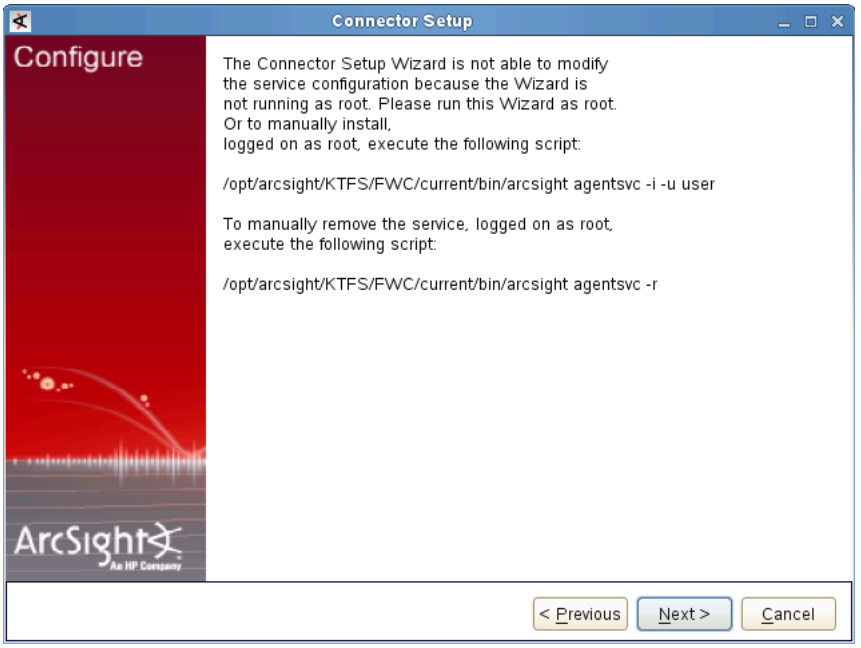


Подробные данные коннектора

Нажмите на кнопку **Next**.

10. Установите службу ArcSight Forwarding Connector.

- Если мастер Connector Setup Wizard запущен без прав root, выводится предупреждение.



Предупреждение о правах пользователя

Можно запустить мастер Connector Setup Wizard как root либо можно выполнить следующую команду как root:

```
%ConnectorInstallDir%/current/bin/arcsight agentsvc -i -u $username -sn $service_name
```

Параметры здесь имеют следующий смысл:

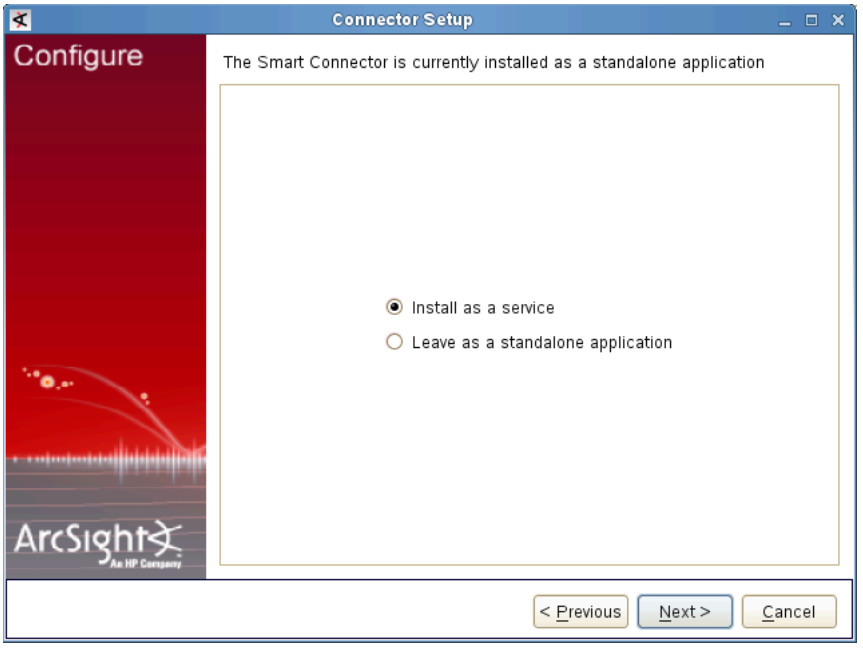
- `$username` — имя пользователя операционной системы, который будет запускать службу.
- `$service_name` — имя службы.

  Рекомендуется задать имя службы таким же, как имя коннектора.

Сообщения о процессе установки выводятся в файл журнала `%ConnectorInstallDir%/current/logs/agent.log`.

Пропустите следующий шаг, описывающий указание параметров службы.

- Если установка запускается от имени пользователя root, выберите **Install as a service**.



Выбор режима установки

Нажмите на кнопку **Next**.

11. Укажите параметры службы.

Рекомендуется задать имя службы таким же, как имя коннектора.



Указание параметров службы

Нажмите на кнопку **Next**.

После этого мастер Connector Setup Wizard сообщит о том, что новый Forwarding Connector установлен.

12. Убедитесь, что коннектор работает (о том, как это делается, см. в разделе об устранении неполадок ArcSight). Если он не запущен, запустите его с помощью следующей команды:

    `/etc/init.d/arc_%FORWARDING% start`

    Где `%FORWARDING%` – это имя коннектора.

Если Forwarding Connector отправляет в Kaspersky CyberTrace Service большое количество событий (более 1000 событий в секунду), рекомендуется сделать следующее: в файле `%ConnectorInstallDir%/current/user/agentagent.wrapper.conf` задать в поле `wrapper.java.maxmemory` значение `512` и перезапустить Forwarding Connector.

Шаг 2 (альтернативный). Установка ArcSight Forwarding Connector с помощью консоли

Для установки ArcSight Forwarding Connector вместо установщика с графическим интерфейсом пользователя можно воспользоваться консолью.

Чтобы установите ArcSight Forwarding Connector с помощью консоли, выполните следующие действия:

1. В консоли запустите установщик ArcSight Forwarding Connector.
2. Прочтите раздел **Introduction** и нажмите клавишу **Enter**.
3. При появлении соответствующего запроса выберите **Choose Install Folder** и введите полный путь к каталогу, в который будет установлен ArcSight Forwarding Connector (`%ConnectorInstallDir%`).

   По умолчанию задан каталог `/root/ArcSightSmartConnectors`.
4. В ответ на запрос выберите **Choose Install Set** и введите `1` (что соответствует варианту `Typical`).

5. При появлении соответствующего запроса выберите **Choose Link Location** и укажите, требуется ли создавать ссылку на каталог установки.

   Рекомендуется выбрать вариант `Don't create links`.

6. Убедитесь, что в разделе **Pre-Installation Summary** указаны правильные значения настроек установки. Если значения правильные, нажмите клавишу **Enter**.

   После установки ArcSight Forwarding Connector в консоли выводится следующая информация:

   ```
   Installation Complete
   ---------------------
   The core components of the ArcSight SmartConnector have been successfully installed to:
   %ConnectorInstallDir%
   To finish the configuration of the SmartAgent, please go to the folder:
   %ConnectorInstallDir%/current/bin/
   and execute the script:
   ./runagentsetup.sh
   ```

7. Запустите скрипт `%ConnectorInstallDir%/current/bin/runagentsetup.sh`.

8. В ответ на запрос выберите `Add a Connector`.

9. Укажите тип соединителя `ArcSight Forwarding Connector`.

10. Укажите, требуется ли маскировать пароли.

    Рекомендуется указать `yes`.

11. Укажите следующие параметры подключения ArcSight Source Manager:

    - **Host Name**

      Хост ArcSight Source Manager.

    - **Port**

      Порт ArcSight Source Manager (по умолчанию `8443`).

    - **User**

      Имя пользователя учетной записи, которую должен использовать ArcSight Forwarding Connector (по умолчанию `FwdCyberTrace`).

      > Вместо `FwdCyberTrace` можно указать другого пользователя. Для этого укажите собственного пользователя ArcSight в настройках ArcSight Forwarding Connector.

    - **Password**

      Пароль от учетной записи, которую должен использовать ArcSight Forwarding Connector (по умолчанию `KasperskyLab!`).

12. Укажите следующее действие для импорта сертификата: `Import the certificate to connector from destination`.

13. Укажите тип назначения: `CEF Syslog`.

14. Задайте следующие параметры:

    - **Ip/Host**

      IP-адрес, который Kaspersky CyberTrace Service прослушивает для получения событий.

    - **Порт**

      Порт на котором Kaspersky CyberTrace Service получает события. По умолчанию это `9999`.

    - **Protocol**

      Укажите `Raw TCP`.

    IP-адрес и порт совпадают с указанными в разделе **Соединение** на вкладке **Служба** в веб-интерфейсе Kaspersky CyberTrace.

15. Задайте следующие настройки коннектора:

    - **Имя**

      Можно указать произвольное значение.

    - **Location**

      Можно указать произвольное значение.

    - **DeviceLocation**

      Можно указать произвольное значение.

    - **Comment**

      Можно указать произвольное значение.

    После этого коннектор регистрируется.

16. Укажите способ установки коннектора: `Install as a service`.

17. Задайте настройки учетной записи:

    - **Service Internal Name**

    - **Service Display Name**

    - **Start the service automatically**

      Задает, должна ли служба запускаться при запуске системы. Рекомендуется указать `yes`.

18. Проверьте указанные данные. Если данные верны, нажмите клавишу **`Enter`**.

    Выполняется установка коннектора как службы.

19. Убедитесь, что коннектор работает (о том, как это делается, см. в разделе об устранении неполадок ArcSight). Если он не запущен, запустите его с помощью следующей команды:

    ```
    /etc/init.d/arc_%FORWARDING% start
    ```

    Где `%FORWARDING%` – это имя коннектора.

Если Forwarding Connector отправляет в Kaspersky CyberTrace Service большое количество событий (более 1000 событий в секунду), рекомендуется сделать следующее: в файле

`%ConnectorInstallDir%/current/user/agentagent.wrapper.conf` задать в поле `wrapper.java.maxmemory` значение `512` и перезапустить Forwarding Connector.

Шаг 3. Настройка Kaspersky CyberTrace для взаимодействия с ArcSight

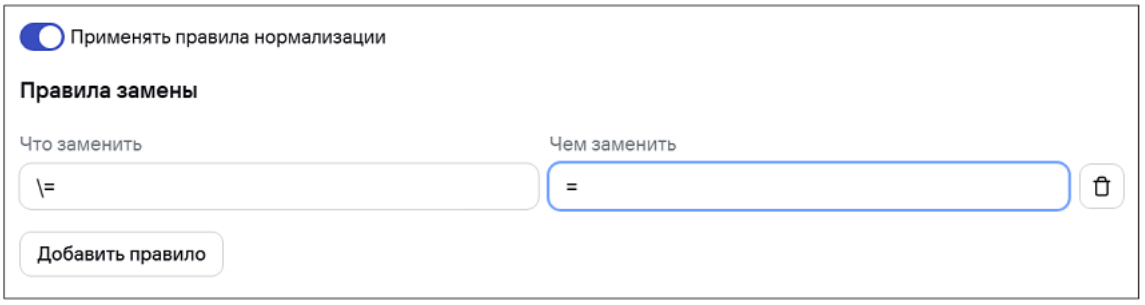
В этом разделе описывается порядок настройки Kaspersky CyberTrace для взаимодействия с ArcSight во время нормальной работы.

Чтобы настроить Kaspersky CyberTrace для взаимодействия с ArcSight, выполните следующие действия:

1. Откройте веб-интерфейс Kaspersky CyberTrace.
2. Перейдите на страницу **Параметры** → **Общие**.
3. В разделе **Входящие события** выберите IP-адрес и порт, которые Kaspersky CyberTrace Service должен прослушивать для получения входящих событий. IP-адрес и порт задаются при установке ArcSight Forwarding Connector (значение по умолчанию `127.0.0.1:9999`).
4. Перейдите на страницу **Параметры** → **Источники событий**.
5. Нажмите на кнопку (**Изменить**) рядом с источником событий **По умолчанию**.

   Откроется окно **Edit event source**.
6. На вкладке **Правила нормализации** выполните следующие действия:
   - В поле **Что заменить** введите последовательность символов `\=`
   - В поле **Чем заменить** введите символ `=`

   После внесения изменений вкладка **Правила нормализации** должна выглядеть следующим образом:



Вкладка **Правила нормализации**.

7. Выберите вкладку **Регулярные выражения**. На этой вкладке содержатся универсальные регулярные выражения, используемые для сопоставления URL (с протоколом), хешей, IP-адресов (источника и назначения), имени устройства, названия производителя, IP-адреса устройства, имени пользователя и идентификатора события. Измените эти регулярные выражения так, чтобы они обеспечивали сопоставление фактических событий.
8. Закройте окно **Edit event source**.
9. На странице **Параметры** → **Служебные оповещения**, введите следующую строку в поле **Формат служебных оповещений**:

   ```
   CEF:0|Kaspersky|Kaspersky CyberTrace for ArcSight|2.0|1|CyberTrace Service Event|4|
   reason=%Alert% msg=%RecordContext%
   ```

10. На странице **Параметры** → **Оповещения об обнаружении индикаторов компрометации** введите следующую строку в поле **Формат оповещения**:

```
CEF:0|Kaspersky|Kaspersky CyberTrace for ArcSight|2.0|2|CyberTrace Detection Event|8|
reason=%Category% dst=%DST_IP% src=%DeviceIp% fileHash=%RE_HASH% request=%RE_URL%
sourceServiceName=%Device% sproc=%Product% suser=%UserName% msg=CyberTrace detected
%Category% externalId=%Id% %ActionableFields% cs5Label=MatchedIndicator
cs5=%MatchedIndicator% cn3Label=Confidence cn3=%Confidence% cs6Label=Context
cs6=%RecordContext%
```

ArcSight и поля контекста

В потоках данных об угрозах Kaspersky Data Feed используются следующие поля контекста (actionable fields). Поля контекста можно просматривать на странице **Параметры** → **Потоки данных**.

- Для потоков данных об угрозах Demo Botnet C&C URL Data Feed и Botnet C&C URL Data Feed:

Field name	Output	Поле CEF
mask	cs1	deviceCustomString1
first_seen	flexString1	flexString1
last_seen	flexString2	flexString2
popularity	cn2	deviceCustomNumber2
threat	cs3	deviceCustomString3
urls/url	cs4	deviceCustomString4
whois/domain	cs2	deviceCustomString2

- Для потоков данных об угрозах Demo Malicious Hash Data Feed и Malicious Hash Data Feed:

Field name	Output	Поле CEF
first_seen	flexString1	flexString1
last_seen	flexString2	flexString2
popularity	cn2	deviceCustomNumber2
threat	cs3	deviceCustomString3
urls/url	cs4	deviceCustomString4
file_size	fsize	file_size

- Для потоков данных об угрозах Demo IP Reputation Feed и IP Reputation Data Feed:

Field name	Output	Поле CEF
first_seen	flexString1	flexString1
last_seen	flexString2	flexString2
popularity	cn2	deviceCustomNumber2
threat_score	cn1	deviceCustomNumber1
domains	cs2	deviceCustomString2
urls/url	cs4	deviceCustomString4
files/threat	cs3	deviceCustomString3

- Для потока данных об угрозах Malicious URL Data Feed:

Field name	Output	Поле CEF
mask	cs1	deviceCustomString1

first_seen	flexString1	flexString1
last_seen	flexString2	flexString2
popularity	cn2	deviceCustomNumber2
files/threat	cs3	deviceCustomString3
category	cs4	deviceCustomString4
whois/domain	cs2	deviceCustomString2

- Для потока данных об угрозах Mobile Malicious Hash Data Feed:

Field name	Output	Поле CEF
first_seen	flexString1	flexString1
last_seen	flexString2	flexString2
popularity	cn2	deviceCustomNumber2
threat	cs3	deviceCustomString3
file_size	fsize	file_size

- Для потока данных об угрозах Phishing URL Data Feed:

Field name	Output	Поле CEF
mask	cs1	deviceCustomString1
first_seen	flexString1	flexString1
last_seen	flexString2	flexString2
popularity	cn2	deviceCustomNumber2
industry	deviceFacility	deviceFacility
whois/domain	cs2	deviceCustomString2

- Для потока данных об угрозах Mobile Botnet Data Feed:

Field name	Output	Поле CEF
threat	cs3	deviceCustomString3

- Для потока данных об угрозах APT URL Data Feed:

Field name	Output	Поле CEF
detection_date	flexString1	flexString1
publication_name	cs3	deviceCustomString3

- Для потока данных об угрозах APT IP Data Feed:

Field name	Output	Поле CEF
detection_date	flexString1	flexString1
publication_name	cs3	deviceCustomString3

- Для потока данных об угрозах APT Hash Data Feed:

Field name	Output	Поле CEF
detection_date	flexString1	flexString1
publication_name	cs3	deviceCustomString3

- Для потока данных об угрозах IoT URL Data Feed:

Field name	Output	Поле CEF
mask	cs1	deviceCustomString1
first_seen	flexString1	flexString1
last_seen	flexString2	flexString2
popularity	cn2	deviceCustomNumber2
files/threat	cs3	deviceCustomString3

Очистка полей ArcSight, заполненных информацией из потоков данных об угрозах Kaspersky Data Feed

Если поле CEF требуется использовать не для информации из потоков данных об угрозах Kaspersky Data Feed, а для какой-либо другой информации, такое поле необходимо очистить.

Чтобы очистить поле CEF, выполните следующие действия:

1. Выберите вкладку **Параметры** веб-интерфейса Kaspersky CyberTrace.
2. Перейдите на страницу **Потоки данных**.
3. Убедитесь, что выбрана вкладка **Лаборатория Касперского**, затем нажмите на тот поток данных об угрозах Kaspersky Threat Data Feeds, который содержит поле, которое требуется очистить.
4. В разделе **Поля контекста** найдите поле **Название выходного поля**, содержащее имя поля CEF, которое требуется очистить.
5. Нажмите на значок удаления ( ) рядом с полем **Название выходного поля**, найденным на предыдущем шаге.

Шаг 4. Проверка работоспособности (ArcSight)

После установки Kaspersky CyberTrace и необходимого программного обеспечения ArcSight можно протестировать их работу.

Прежде чем редактировать какие-либо правила фильтрации в конфигурационном файле Feed Utility, следует обязательно выполнить проверку работоспособности.

Чтобы проверить, правильно ли Kaspersky CyberTrace интегрирован с ArcSight, выполните следующие действия:

1. Настройте Log Scanner для отправки событий в ArcSight SmartConnector.

   Для этого задайте хост и порт ArcSight SmartConnector в элементе `Connection` конфигурационного файла Log Scanner.

2. Отправьте файл `%service_dir%/verification/kl_verification_test_cef.txt` в ArcSight SmartConnector.

   Для этого выполните следующую команду (в Linux):

   ```
   ./log_scanner -p ../verification/kl_verification_test_cef.txt
   ```

   Для этого выполните следующую команду (в Windows):

   ```
   log_scanner.exe -p ..\verification\kl_verification_test_cef.txt
   ```

Не указывайте в этой команде флаг `-r` — отправлять результаты проверки в SIEM-систему с использованием параметров для исходящих событий, указанных в разделе Service настроек Kaspersky CyberTrace.

3. Убедитесь, что полученные результаты проверки соответствуют приведенным ниже.

   Результаты проверки можно просмотреть в активном канале **CyberTrace all matches**. Для этого в поле **Source Service Name** задайте следующий встроенный фильтр: `Kaspersky Lab|CyberTrace Verification Kit`.

Результаты проверки работоспособности

Результаты проверки работоспособности зависят от используемых потоков данных об угрозах. Результаты проверки работоспособности приведены в следующей таблице.

Результаты проверки работоспособности

Используемый поток данных об угрозах	Обнаруженные объекты
Malicious URL Data Feed	http://fakess123.nu http://badb86360457963b90faac9ae17578ed.com
Phishing URL Data Feed	http://fakess123ap.nu http://e77716a952f640b42e4371759a661663.com
Botnet C&C URL Data Feed	http://fakess123bn.nu http://a7396d61caffe18a4cffbb3b428c9b60.com
IP Reputation Data Feed	192.0.2.0 192.0.2.3
Malicious Hash Data Feed	FEAF2058298C1E174C2B79AFFC7CF4DF 44D88612FEA8A8F36DE82E1278ABB02F (EICAR Standard Anti-Virus Test File) C912705B4BBB14EC7E78FA8B370532C9
Mobile Malicious Hash Data Feed	60300A92E1D0A55C7FDD360EE40A9DC1
Mobile Botnet C&C URL Data Feed	001F6251169E6916C455495050A3FB8D (хеш MD5) sdfed7233dsfg93acvbhl.su/steallallsms.php (маска URL)
Ransomware URL Data Feed	http://fakess123r.nu http://fa7830b4811fbef1b187913665e6733c.com
APT URL Data Feed	http://b046f5b25458638f6705d53539c79f62.com
APT Hash Data Feed	7A2E65A0F70EE0615EC0CA34240CF082
APT IP Data Feed	192.0.2.4
IoT URL Data Feed	http://e593461621ee0f9134c632d00bf108fd.com/.i
Demo Botnet C&C URL Data Feed	http://5a015004f9fc05290d87e86d69c4b237.com http://fakess123bn.nu
Demo IP Reputation Data Feed	192.0.2.1 192.0.2.3
Demo Malicious Hash Data Feed	776735A8CA96DB15B422879DA599F474 FEAF2058298C1E174C2B79AFFC7CF4DF 44D88612FEA8A8F36DE82E1278ABB02F
ICS Hash Data Feed	7A8F30B40C6564EFF95E678F7C43346C

Указание собственного пользователя ArcSight в настройках ArcSight Forwarding Connector

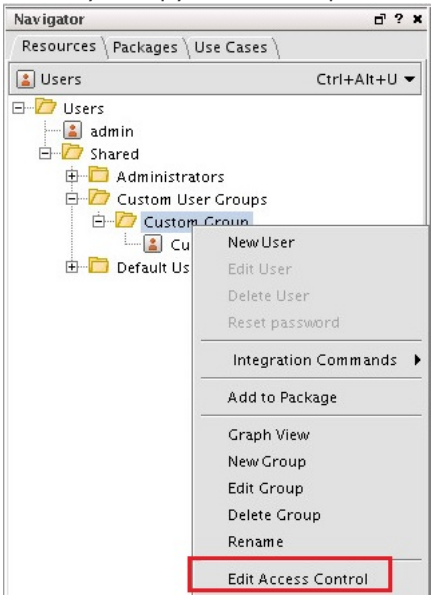
В этом разделе описывается порядок указания собственного пользователя ArcSight в настройках ArcSight Forwarding Connector.

При импорте пакета ARB в ArcSight пользователь создается пользователь `FwdCyberTrace` в группе `Kaspersky CyberTrace Connector`. Эта учетная запись пользователя предназначена для использования в ArcSight Forwarding Connector. Вместо этой учетной записи пользователя можно создать другую. В этом случае рекомендуется удалить пользователя `FwdCyberTrace` и группу `Kaspersky CyberTrace Connector`. Обратите внимание, что создаваемый собственный пользователь должен иметь тип Forwarding Connector.

Чтобы создать собственную учетную запись пользователя ArcSight для пересылки событий из ArcSight ESM в Kaspersky CyberTrace Service, выполните следующие действия:

1. Запустите ArcSight Console.
2. На панели **Navigator** выберите вкладку **Resources**.
3. Откройте раскрывающийся список и выберите **Users**.
4. В дереве выберите группу пользователей, содержащую созданную собственную учетную запись.

   Рекомендуется поместить этого пользователя в отдельную группу пользователей, созданную только для этого пользователя.
5. В дереве щелкните правой кнопкой мыши пункт группы и выберите **Edit Access Control**.



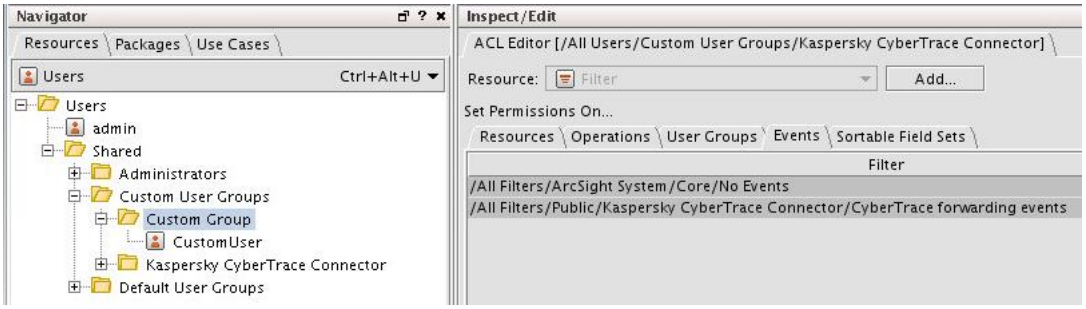
Изменение настроек доступа

6. На панели **Inspect/Edit** выберите вкладку **Events**.
7. Нажмите на кнопку **Add**.

8. Выберите следующие фильтры событий:

   - `CyberTrace forwarding events`

     Это фильтр для событий, содержащих хеши, URL и IP-адреса.



Выбор фильтров событий

9. Установите или перенастройте ArcSight Forwarding Connector.

   Процедура перенастройки ArcSight Forwarding Connector описана ниже в этом разделе.

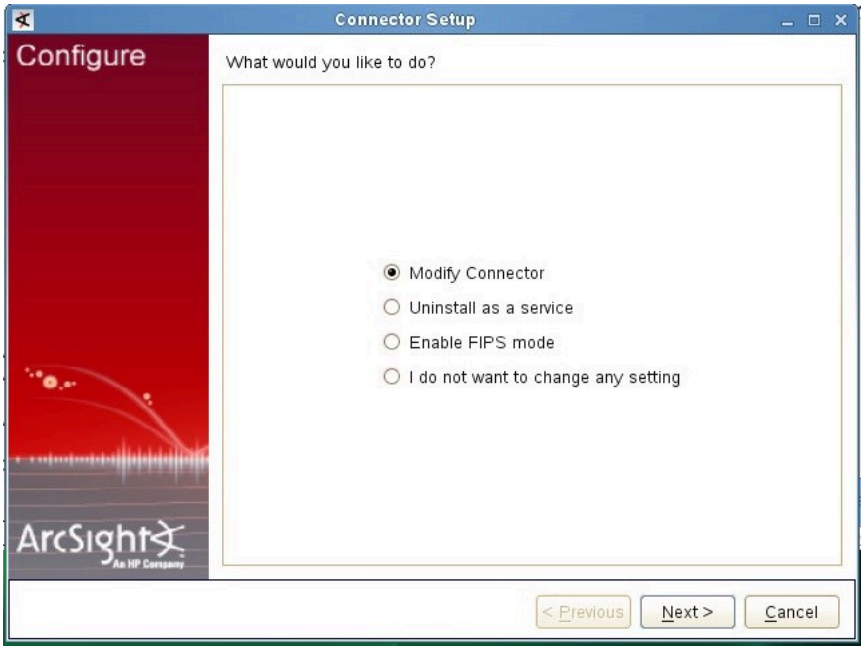
Чтобы изменить конфигурацию ArcSight Forwarding Connector, выполните следующие действия:

1. Измените текущий рабочий каталог на `%FORWARDING_DIR%/current/bin`.

   Здесь `%FORWARDING_DIR%` — каталог, в который установлен ArcSight Forwarding Connector.

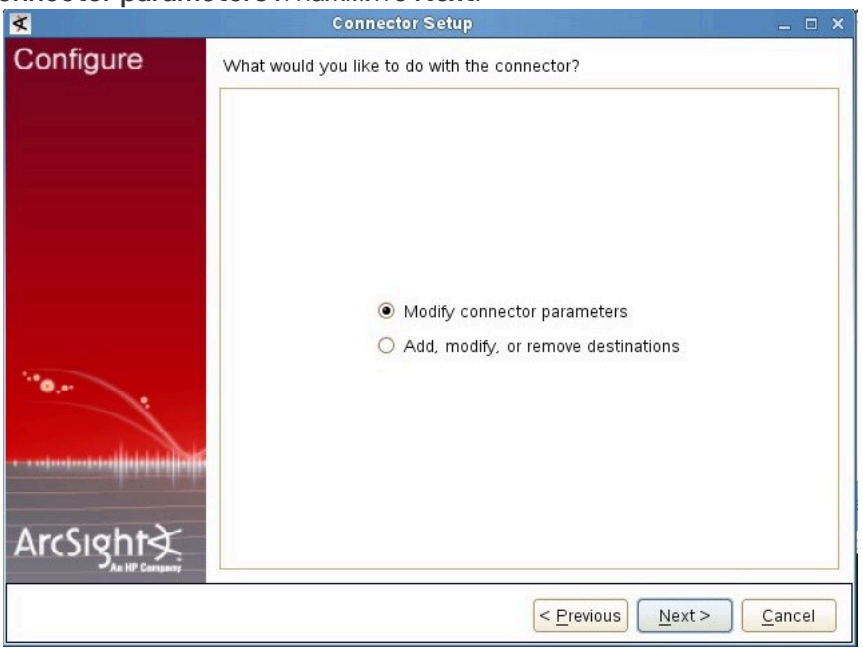
2. Запустите скрипт runagentsetup.sh.

3. Выберите **Modify Connector** и нажмите **Next**.



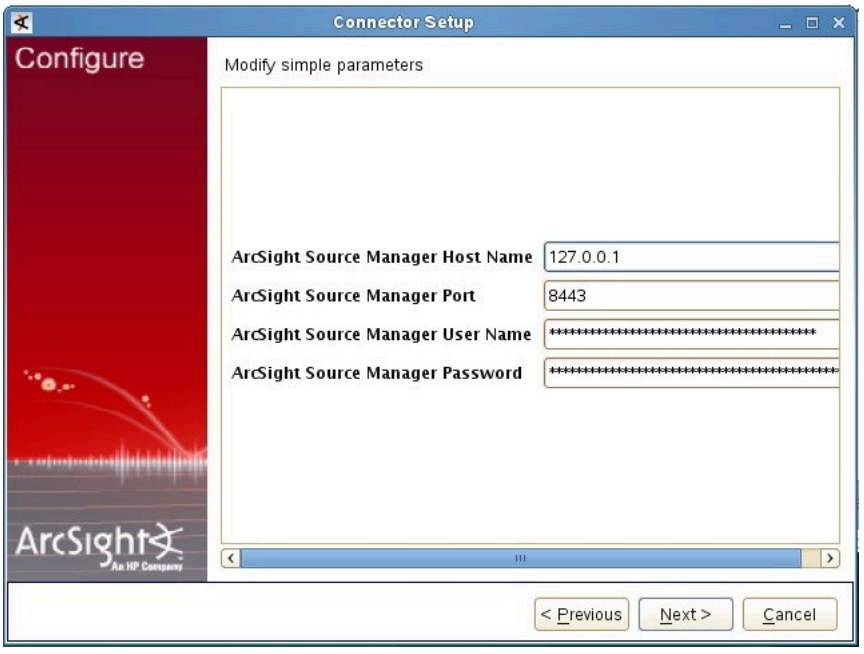
Изменение коннектора

4. Выберите **Modify connector parameters** и нажмите **Next**.



Изменение параметров коннектора

5. Задайте параметры ArcSight и учетные данные созданной собственной учетной записи, затем нажмите **Next**.



Указание параметров ArcSight Source Manager

6. Нажмите **Next**, затем нажмите **Finish**, чтобы завершить работу с окном **Connector Setup**.

Интеграция с QRadar

В этой главе описывается порядок интеграции Kaspersky CyberTrace с QRadar.

Стандартная интеграция (QRadar)

В этом разделе описывается порядок интеграции Kaspersky CyberTrace и QRadar по стандартной схеме интеграции.

Используйте этот сценарий, если есть возможность получать обновления QRadar.

О стандартной схеме интеграции (QRadar)

В этом разделе описывается стандартная схема интеграции QRadar и Kaspersky CyberTrace.

Для корректной работы стандартной схемы интеграции необходимо установить обновление DSM-KasperskyCyberTrace-%version%-20180802144954.noarch.rpm, где `%version%` соответствует версии QRadar. Обычно эти обновления поставляются в процессе автоматического обновления, но вы также можете загрузить их вручную с сайта IBM Fix Central.

О компонентах стандартной схемы интеграции

В стандартной схеме интеграции QRadar используются следующие компоненты:

- Kaspersky CyberTrace Service

  Эта служба сопоставляет события QRadar с потоками данных об угрозах Kaspersky Threat Data Feeds.

- QRadar

  SIEM-система, используемая в этой интеграции.

- Средства контроля безопасности

  Это источники событий для QRadar, такие как межсетевые экраны, прокси-серверы, системы обнаружения вторжений и другие сетевые устройства.

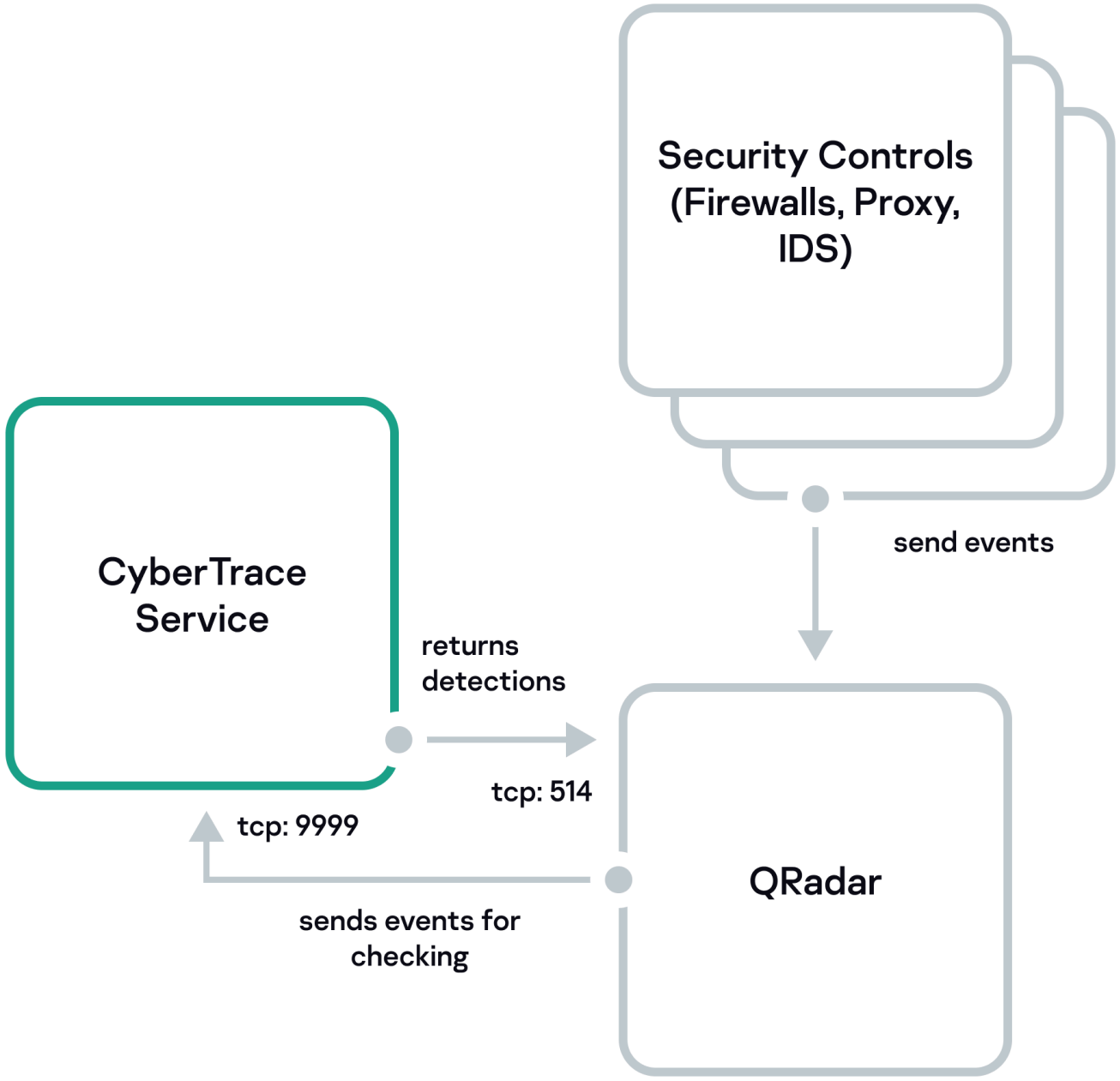
  Средства контроля безопасности могут отправлять события в QRadar любым способом, поддерживаемым QRadar.

Стандартная схема интеграции

В стандартной схеме интеграции Kaspersky CyberTrace Service по умолчанию настраивается на прослушивание адреса `0.0.0.0:9999` (все интерфейсы) для получения входящих событий от QRadar.

Kaspersky CyberTrace Service отправляет события обнаруженных киберугроз на порт 514 интерфейса, определенного в конфигурации QRadar. Адрес этого интерфейса указывается при установке Kaspersky CyberTrace.

Средства контроля безопасности могут отправлять события в QRadar в любом формате, поддерживаемом QRadar, например, Syslog, JDBC, OPSEC, File или SNMP.



Стандартная схема интеграции для QRadar

Шаг 1. Настройка QRadar для получения последних обновлений

В этом разделе описывается порядок получения последних обновлений QRadar.

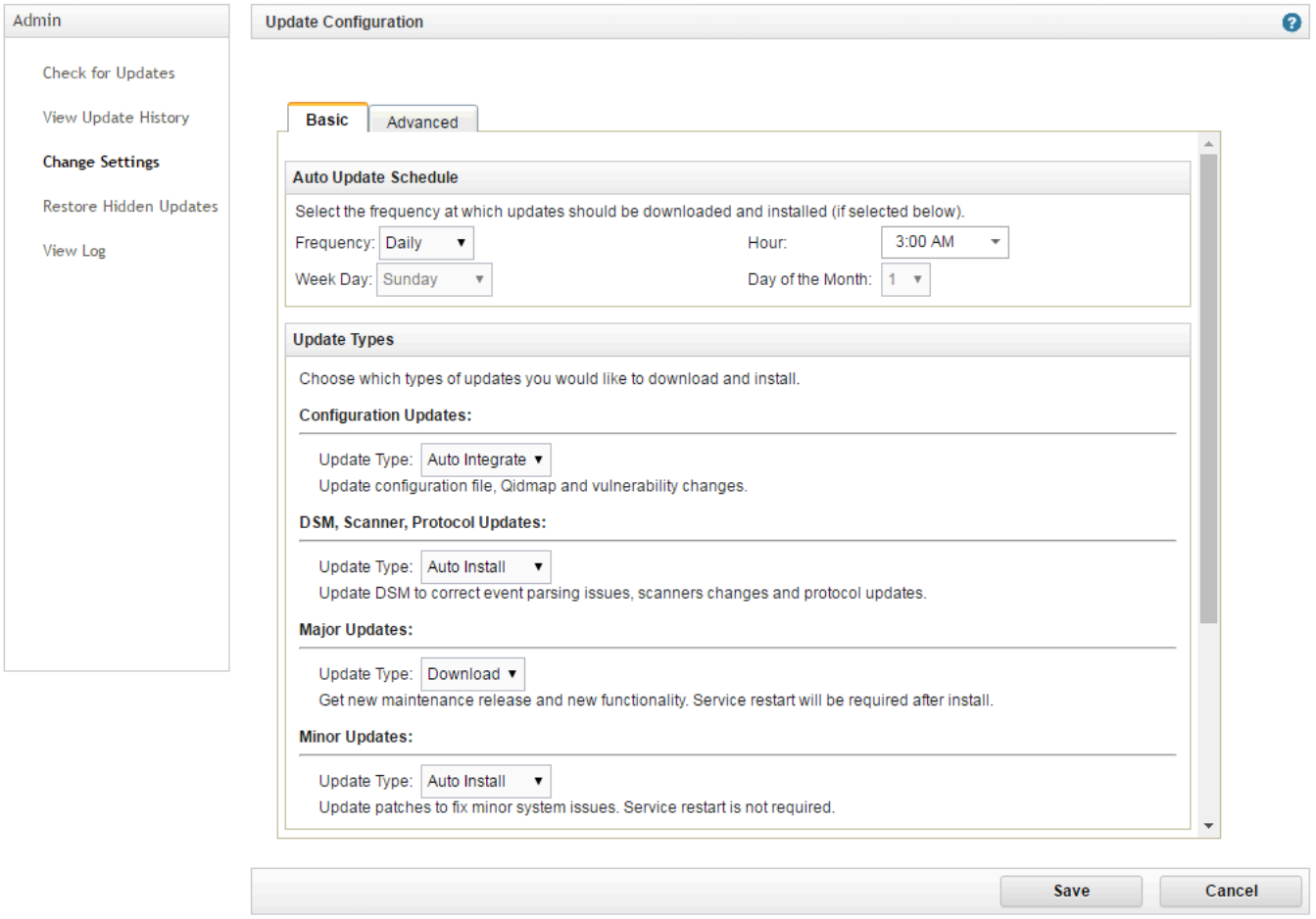
Чтобы настроить QRadar для получения последних обновлений, выполните следующие действия:

1. В QRadar Console выберите **Admin** → **Auto-Update**.

   Откроется форма **Update Configuration**.

2. На вкладке **Basic**, в разделе **Configuration Updates** в раскрывающемся списке **Update Type** выберите **Auto Integrate**.

3. В разделе **DSM, Scanner, Protocol Updates** выберите тип обновления **Auto Install**.



Обновите конфигурацию

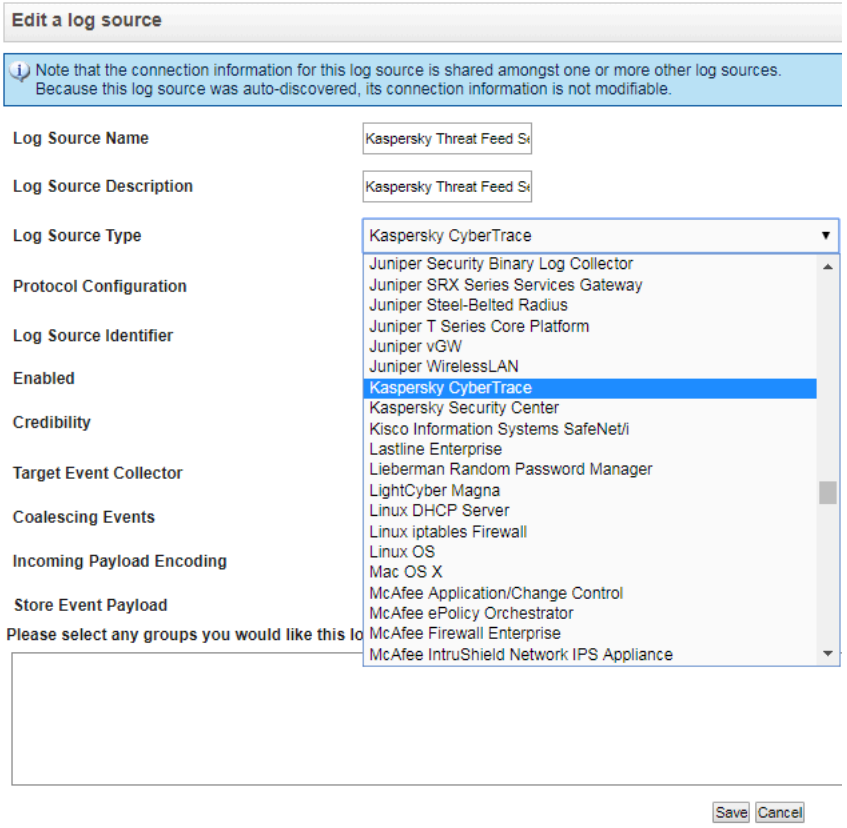
4. Нажмите на кнопку **Save**.

5. Дождитесь установки обновлений.

6. В QRadar Console выберите **Admin** → **Log Sources** → **Add**.

   Откроется форма **Add a log source**.

7. Убедитесь, что `Kaspersky CyberTrace` отображается в раскрывающемся списке **Log Source Type**.



Тип источника журналов Kaspersky CyberTrace

В качестве альтернативы автоматическому обновлению QRadar можно воспользоваться сайтом IBM Fix Central и вручную загрузить и установить пакет DSM, указанный в разделе О стандартной схеме интеграции (QRadar), а затем настроить QRadar, как описано в разделе Интеграция с QRadar в случае, если QRadar не может получать обновления.

Шаг 2. Отправка набора событий в QRadar

На этом шаге необходимо отправить в QRadar два набора событий, чтобы QRadar автоматически добавил два новых источника журналов — один для проверки работоспособности, а другой — для событий из Kaspersky CyberTrace Service.

Чтобы добавить новые источники журналов, выполните следующие действия:

1. Отправьте файл журнала проверки работоспособности.

   Отправьте в QRadar файл `verification/kl_verification_test_leef.txt`, как описано в подразделе «Отправка набора событий» ниже.

   После отправки файла проверки работоспособности QRadar будет содержать источник журналов `KL_Verification_Tool`.

2. Отправьте образец файла журнала.

   Для тестирования и окончательной настройки интеграции с QRadar отправьте образец файла журнала `integration/qradar/sample_initiallog.txt` в QRadar, как описано в подразделе «Отправка набора событий» ниже.

   После отправки образца файла журнала QRadar будет содержать источник журналов `KL_Feed_Service_v2`.

Согласно документации QRadar, после добавления нового источника журналов может быть пропущено до 25 событий. Таким образом, возможно, файл sample_initiallog.txt придется отправить несколько раз. Таким образом будет обеспечено отображение некоторых событий в QRadar и их обработка в Kaspersky CyberTrace Service.

Отправка набора событий

Чтобы отправить события в QRadar, выполните следующие действия:

1. В элементе `Connection` конфигурационного файла Log Scanner укажите IPv4-адрес и порт сервера QRadar (обычно это `514`).

2. Вызовите следующую команду из каталога Log Scanner:

   В ОС Linux:

   ```
   ./log_scanner -p <log_file> [-p <log_file2> ...]
   ```

   В ОС Windows:

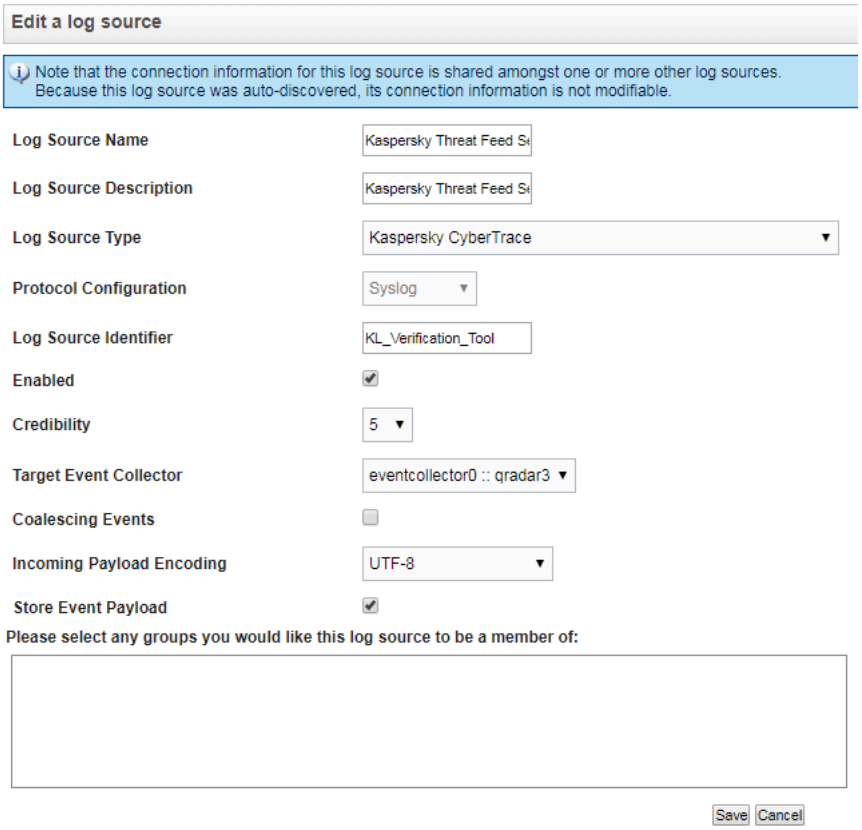
   ```
   log_scanner.exe -p <log_file> [-p <log_file2> ...]
   ```

   `<log_file>`, `<log_file2>` – отправляемые файлы журналов. Кроме того, можно указать каталог, содержащий файлы журнала для отправки.

3. В QRadar Console (т. е. в веб-интерфейсе QRadar) выберите **Admin** → **Log Sources**.

   В списке источников журналов появится новый источник журналов типа `Kaspersky CyberTrace`.

4. В форме настроек нового источника журналов снимите флажок **Coalescing Events**, затем нажмите кнопку **Save**.



Редактирование источника журналов

5. При необходимости выполните развертывание изменений, для этого выберите пункт меню **Admin** → **Deploy Changes** в QRadar Console.

Если события не поступают на порт 514 сервера QRadar, выполните следующие команды с хоста, на котором установлен QRadar.

Выполните команду для консоли QRadar и подождите пять минут:

```
/opt/qradar/support/all_servers.sh -Ck 'if [ -f /opt/qradar/ecs/license.txt ] ; then echo
-n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" >
/opt/qradar/ecs/license.txt ; fi ; if [ -f /opt/ibm/si/services/ecs-ec-
ingress/current/eventgnosis/license.txt ] ; then echo -n "QRadar:Q1 Labs
Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/ibm/si/services/ecs-ec-
ingress/current/eventgnosis/license.txt ; fi ; if [ -f /opt/ibm/si/services/ecs-
ep/current/eventgnosis/license.txt ] ; then echo -n "QRadar:Q1 Labs
Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/ibm/si/services/ecs-
ep/current/eventgnosis/license.txt ; fi ; if [ -f /opt/ibm/si/services/ecs-
ec/current/eventgnosis/license.txt ] ; then echo -n "QRadar:Q1 Labs
Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/ibm/si/services/ecs-
ec/current/eventgnosis/license.txt ; fi ; if [ -f /usr/eventgnosis/ecs/license.txt ] ;
then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" >
/usr/eventgnosis/ecs/license.txt ; fi ; if [ -f
/opt/qradar/conf/templates/ecs_license.txt ] ; then echo -n "QRadar:Q1 Labs
Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" >
/opt/qradar/conf/templates/ecs_license.txt ; fi'
```

Выполните команду для QRadar Community Edition и подождите пять минут:

```
if [ -f /opt/qradar/ecs/license.txt ] ; then echo -n "QRadar:Q1 Labs
Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/qradar/ecs/license.txt ; fi ;
if [ -f /opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/license.txt ] ; then echo
-n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" >
/opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/license.txt ; fi ; if [ -f
/opt/ibm/si/services/ecs-ep/current/eventgnosis/license.txt ] ; then echo -n "QRadar:Q1
Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/ibm/si/services/ecs-
ep/current/eventgnosis/license.txt ; fi ; if [ -f /opt/ibm/si/services/ecs-
ec/current/eventgnosis/license.txt ] ; then echo -n "QRadar:Q1 Labs
Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/ibm/si/services/ecs-
ec/current/eventgnosis/license.txt ; fi ; if [ -f /usr/eventgnosis/ecs/license.txt ] ;
then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" >
/usr/eventgnosis/ecs/license.txt ; fi ; if [ -f
/opt/qradar/conf/templates/ecs_license.txt ] ; then echo -n "QRadar:Q1 Labs
Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" >
/opt/qradar/conf/templates/ecs_license.txt ; fi
```

Шаг 3. Пересылка событий из QRadar в Kaspersky CyberTrace Service

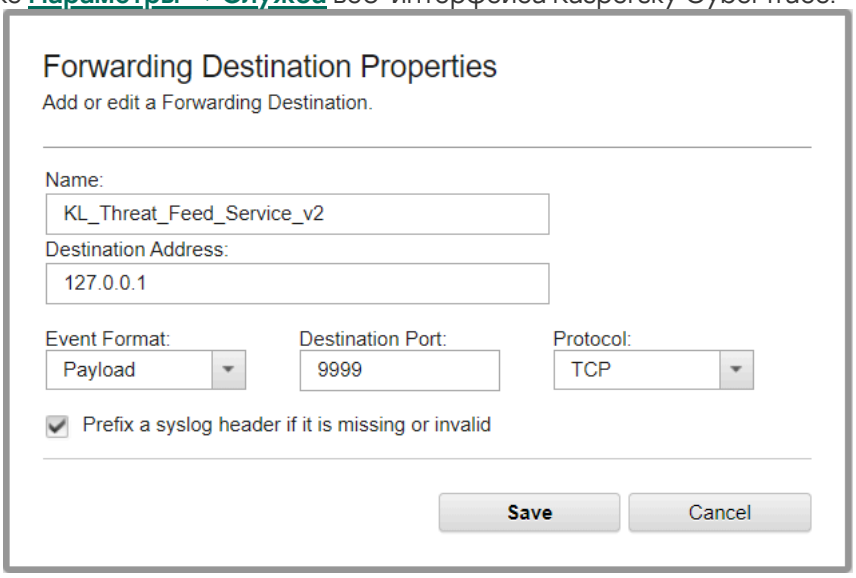
Чтобы проверять события, поступающие в QRadar, через Kaspersky CyberTrace Service, необходимо настроить в QRadar пересылку событий в Kaspersky CyberTrace Service.

Чтобы пересылать события из QRadar в Kaspersky CyberTrace Service, выполните следующие действия:

1. Выберите **Admin** → **System Configuration** → **Forwarding Destinations** → **Add**.
2. В окне **Forwarding Destination Properties** введите идентификатор места точки назначения (например, `"KL_Threat_Feed_Service_v2"`).
3. Введите адрес назначения (хост, на котором запущен Kaspersky CyberTrace Service).
4. Выберите формат событий `Payload` и протокол `TCP`.

> Формат `Payload` может содержать меньше информации по сравнению с форматом `JSON`. Например, если используются имена источников событий, QRadar может удалять их из события. Вместо этого можно указать формат `JSON`, однако его важно правильно настроить. Инструкция по настройке событий в формате `JSON` для пересылки в Kaspersky CyberTrace приведена в подразделе «Рекомендации по настройке событий в формате JSON» ниже.

5. Задайте порт в соответствии с параметрами входящих событий Kaspersky CyberTrace. Эта информация приведена на вкладке **Параметры → Служба** веб-интерфейса Kaspersky CyberTrace.



Добавление назначения пересылки

6. Нажмите на кнопку **Save**.

7. Выберите **Admin** → **Routing rules** → **Add**.

8. В окне **Routing Rule** введите имя правила (например, `KL_Threat_Feed_Service_v2_Rule`).

9. Выберите режим `Online`.

10. Оставьте значение по умолчанию в раскрывающемся списке **Forwarding Event Collector**.

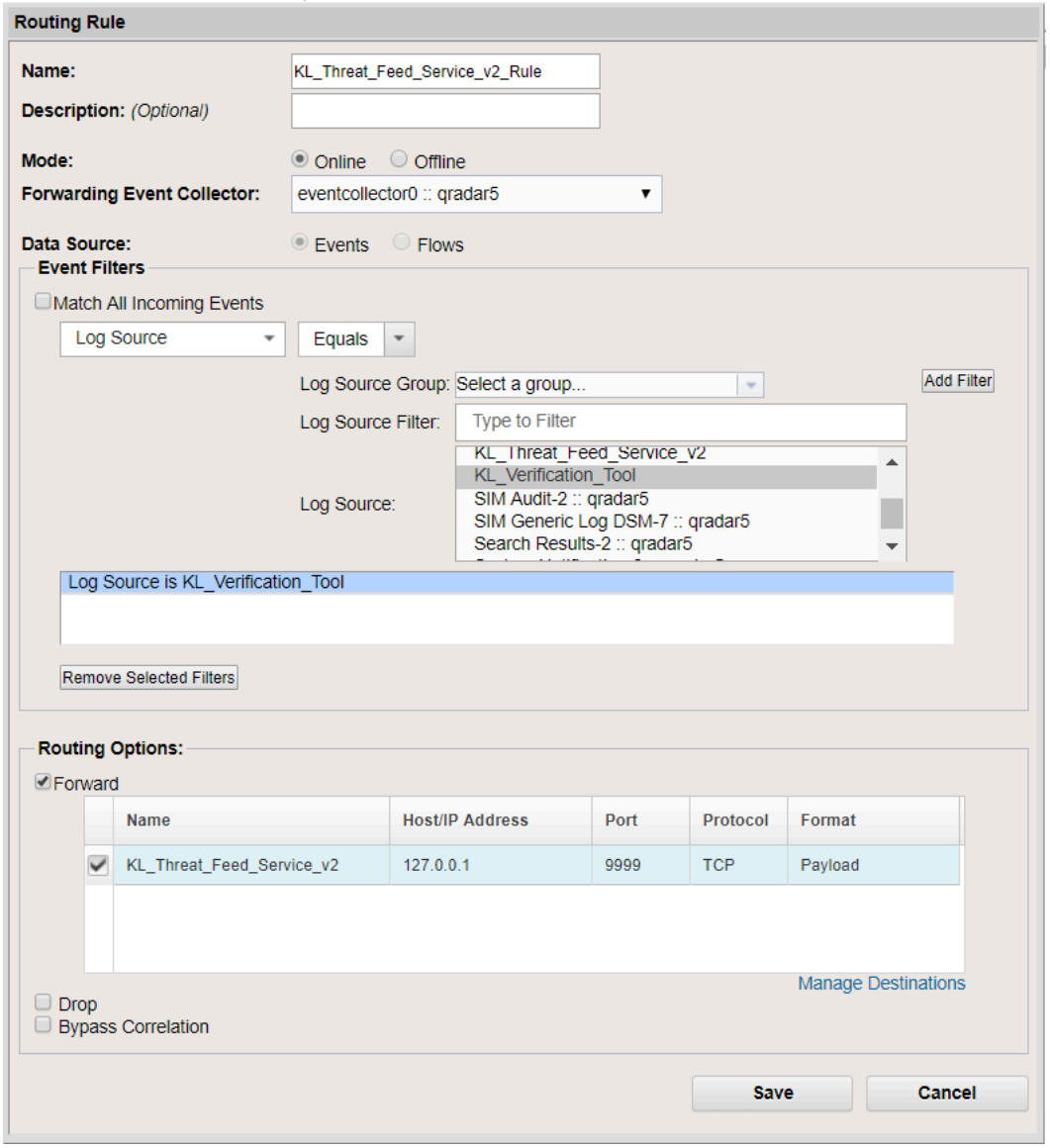
11. Выберите `Events` в качестве источника данных.

12. В группе **Event Filters** задайте фильтр событий.

    Выберите источники журналов вместе с `KL_Verification_Tool` и используйте оператор `Equals any of` в фильтре. Кроме того, для достижения максимальной производительности службы рекомендуется выбирать только те события, которые содержат индикаторы для поиска в потоках данных об угрозах (например, URL, хеши (MD5, SHA1, SHA256) и IP-адреса).

    Снимите или оставьте снятым флажок **Match all incoming events**, чтобы события обнаруженных киберугроз, полученные от Kaspersky CyberTrace Service, не отправлялись обратно в Kaspersky CyberTrace Service.

13. Установите флажок **Forward**. В таблице рядом с столбцом **Name** установите флажок рядом с элементом, добавленным на шаге 1 (в данном случае это `KL_Threat_Feed_Service_v2`).



Добавление правила маршрутизации

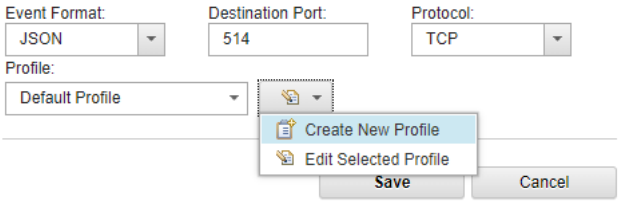
14. Нажмите на кнопку **Save**.

Рекомендации по настройке событий в формате JSON

Некоторые версии QRadar (например, 7.3.2 Patch 6 и 7.4.0) могут отбрасывать некоторые пересылаемые события в формате `JSON`, что может привести к некорректным результатам. Чтобы этого не происходило, рекомендуется исключить некоторые поля из события в формате `JSON` (для получения полного списка таких полей обратитесь в службу поддержки IBM QRadar или попытайтесь определить этот список вручную). В веб-интерфейсе Kaspersky CyberTrace необходимо указать дополнительные правила нормализации (см. ниже).

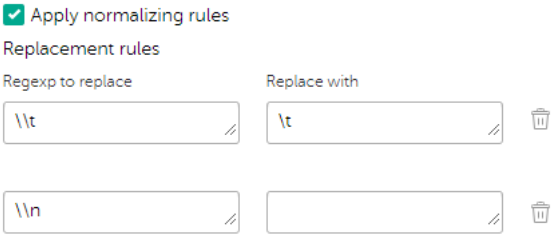
Поэтому формат `JSON` следует использовать вместо формата `Payload`, если событие в формате `Payload` не содержит необходимых полей. В таком случае следует убедиться, что выполняются следующие условия:

- В окне **Forwarding Destination Properties** выбраны только необходимые поля. QRadar не отбрасывает пересылаемые события. Чтобы включить или отключить поля, пересылаемые в рамках события, откройте окно **Forwarding Profile Properties**, нажав на кнопку рядом с полем **Профиль**.



Настройка событий в формате JSON

- На вкладке **Параметры** → **Источники событий** веб-интерфейса Kaspersky CyberTrace заданы следующие правила нормализации:



Настройка дополнительных правил нормализации

Шаг 4. Проверка работоспособности (QRadar)

В этом разделе описывается порядок проверки возможностей Kaspersky CyberTrace с помощью проверки работоспособности.

> Перед изменением каких-либо настроек процесса сопоставления необходимо выполнить проверку работоспособности.

Что такое проверка работоспособности

Проверка работоспособности — это процедура, позволяющая проверить возможности Kaspersky CyberTrace и убедиться в корректности интеграции.

В ходе проверки проверяется, поступают ли события из QRadar в Kaspersky CyberTrace Service, поступают ли события из Kaspersky CyberTrace Service в QRadar, и корректно ли проходит парсинг событий в Kaspersky CyberTrace Service с использованием регулярных выражений.

> События могут не поступать на порт 514 сервера QRadar. Порядок разрешения этой проблемы приведен в разделе Отправка набора событий в QRadar.

О файле для проверки работоспособности

Файл для проверки работоспособности — это файл, содержащий набор событий с URL, IP-адресами и хешами. Этот файл находится в комплекте поставки в каталоге `./verification`. Имя файла — `kl_verification_test_leef.txt`.

Порядок проверки работоспособности

Для проверки работоспособности установленного программного обеспечения, выполните следующие действия:

1. Убедитесь, что в QRadar добавлен источник журнала `KL_Verification_Tool` и правила маршрутизации настроены таким образом, что события из `KL_Verification_Tool` отправляются в Kaspersky CyberTrace Service.

2. Откройте QRadar Console и выберите вкладку **Log Activity**.

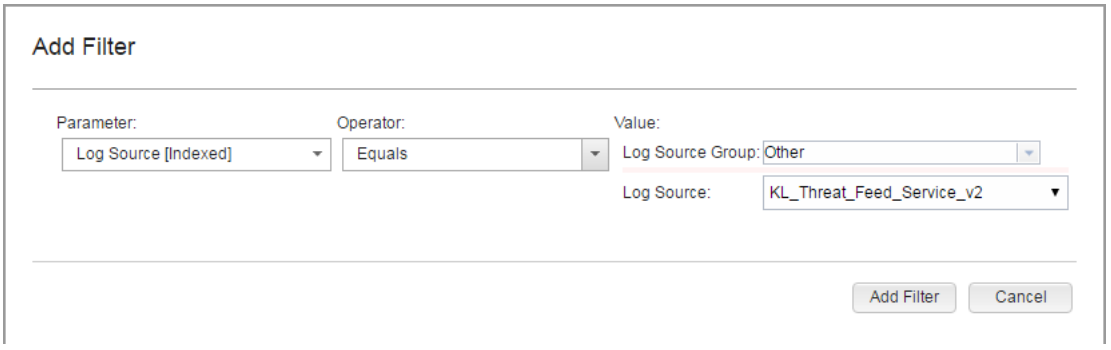
3. Добавьте фильтр:

   a. Нажмите на кнопку **Add Filter**.

   b. В раскрывающемся списке **Parameter** выберите `Log Source`.

   c. В раскрывающемся списке **Operator** выберите `Equals`.

   d. В группе **Value** в раскрывающемся списке **Log Source** выберите требуемое имя службы.



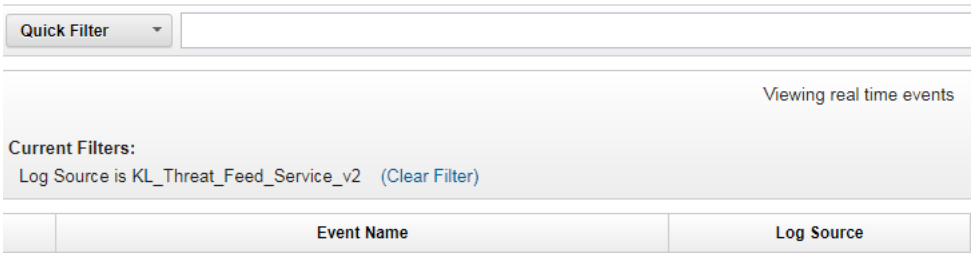
Добавление фильтра для просмотра событий

   a. Нажмите на кнопку **Add Filter**.

   В разделе **Current Filters** отображается строка `Log Source is KL_Threat_Feed_Service_v2`.

4. В раскрывающемся списке **View** выберите `Real Time`, чтобы очистить область событий.

   Теперь можно просматривать информацию о служебных событиях.



Просмотр отфильтрованной информации

5. Отправьте файл `kl_verification_test_leef.txt` в QRadar с помощью Log Scanner, для этого выполните следующую команду:

   В ОС Linux: `./log_scanner -p ../verification/kl_verification_test_leef.txt`

   В ОС Windows: `log_scanner.exe -p ..\verification\kl_verification_test_leef.txt`

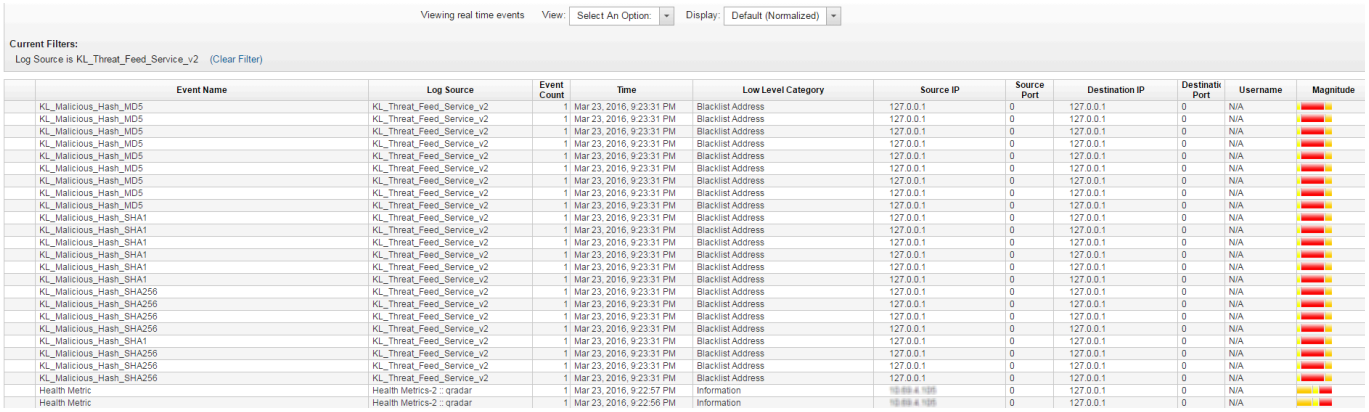
Если в этой команде указан флаг `-r`, результаты проверки будут записаны в файл отчета Log Scanner. Если флаг `-r` не указан, результаты проверки отправляются в SIEM-систему с использованием настроек исходящих событий, заданных для Kaspersky CyberTrace Service.

Ожидаемые результаты, которые должны отображаться в QRadar, зависят от используемых потоков данных об угрозах. Результаты проверки работоспособности приведены в следующей таблице.

Результаты проверки работоспособности

Используемый поток данных об угрозах	Обнаруженные объекты
Malicious URL Data Feed	http://fakess123.nu http://badb86360457963b90faac9ae17578ed.com
Phishing URL Data Feed	http://fakess123ap.nu http://e77716a952f640b42e4371759a661663.com
Botnet C&C URL Data Feed	http://fakess123bn.nu http://a7396d61caffe18a4cffbb3b428c9b60.com
IP Reputation Data Feed	192.0.2.0 192.0.2.3
Malicious Hash Data Feed	FEAF2058298C1E174C2B79AFFC7CF4DF 44D88612FEA8A8F36DE82E1278ABB02F (EICAR Standard Anti-Virus Test File) C912705B4BBB14EC7E78FA8B370532C9
Mobile Malicious Hash Data Feed	60300A92E1D0A55C7FDD360EE40A9DC1
Mobile Botnet C&C URL Data Feed	001F6251169E6916C455495050A3FB8D (хеш MD5) http://sdfed7233dsfg93acvbhl.su/steallallsms.php (маска URL)
Ransomware URL Data Feed	http://fakess123r.nu http://fa7830b4811fbef1b187913665e6733c.com
APT URL Data Feed	http://b046f5b25458638f6705d53539c79f62.com
APT Hash Data Feed	7A2E65A0F70EE0615EC0CA34240CF082
APT IP Data Feed	192.0.2.4
IoT URL Data Feed	http://e593461621ee0f9134c632d00bf108fd.com/.i
Demo Botnet C&C URL Data Feed	http://5a015004f9fc05290d87e86d69c4b237.com http://fakess123bn.nu
Demo IP Reputation Data Feed	192.0.2.1 192.0.2.3

Demo Malicious Hash Data Feed	776735A8CA96DB15B422879DA599F474 FEAF2058298C1E174C2B79AFFC7CF4DF 44D88612FEA8A8F36DE82E1278ABB02F
ICS Hash Data Feed	7A8F30B40C6564EFF95E678F7C43346C



Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destinatic Port	Username	Magnitude
KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_SHA1	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_SHA1	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_SHA1	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_SHA1	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_SHA1	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_SHA1	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_SHA256	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_SHA256	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_SHA256	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_SHA256	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_SHA1	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_SHA256	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_SHA256	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
KL_Malicious_Hash_SHA256	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address	127.0.0.1	0	127.0.0.1	0	N/A	
Health Metric	Health Metrics-2 :: qradar	1	Mar 23, 2016, 9:22:57 PM	Information	[redacted]	0	127.0.0.1	0	N/A	
Health Metric	Health Metrics-2 :: qradar	1	Mar 23, 2016, 9:22:56 PM	Information	[redacted]	0	127.0.0.1	0	N/A	

Просмотр событий из Kaspersky CyberTrace Service

Если фактические результаты проверки совпадают с ожидаемыми, интеграция Kaspersky CyberTrace Service с QRadar работает корректно.

Шаг 5. Получение свойств пользовательского события

В этом разделе описывается порядок настройки извлечения из исходящих событий Kaspersky CyberTrace пользовательских свойств событий в дополнение к стандартным полям. В результате настройки выполняется извлечение хешей MD5, SHA1 и SHA256, а правило извлечения «Source IP» переопределяется.

Чтобы настроить получение пользовательских свойств события, выполните следующие действия:

1. Выберите вкладку **Log Activity**, затем нажмите **Add Filter**.

   Откроется форма **Add Filter**.

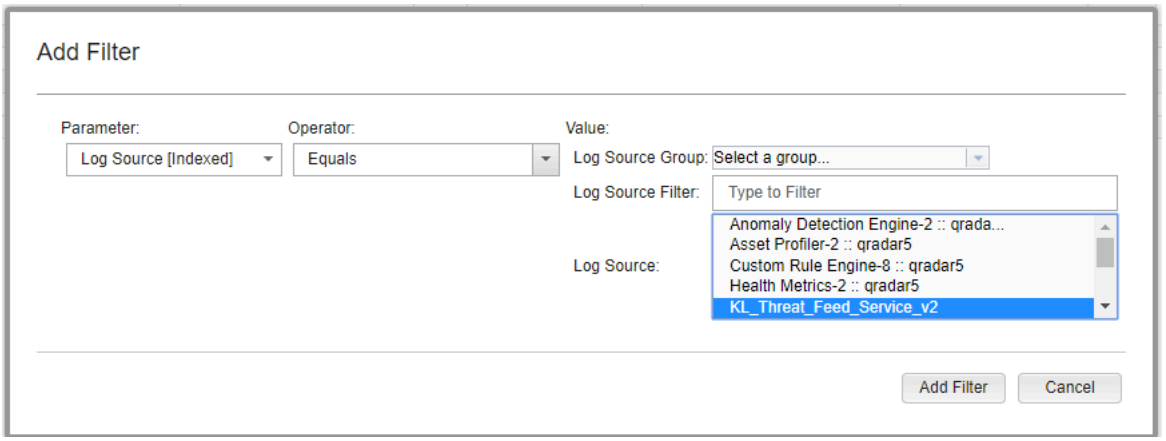
2. Заполните эту форму:

   a. В раскрывающемся списке **Parameter** выберите `Log Source [Indexed]`.

   b. В раскрывающемся списке **Operator** выберите `Equals`.

c. В списке **Log Source** выберите `KL_Threat_Feed_Service_v2`.

Вариант выбора `KL_Threat_Feed_Service_v2` соответствует имени источника журналов, заданному в элементе `OutputSettings > EventFormat` и в элементе `OutputSettings > AlertFormat` конфигурационного файла Kaspersky CyberTrace (их также можно задать с помощью веб-интерфейса Kaspersky CyberTrace).

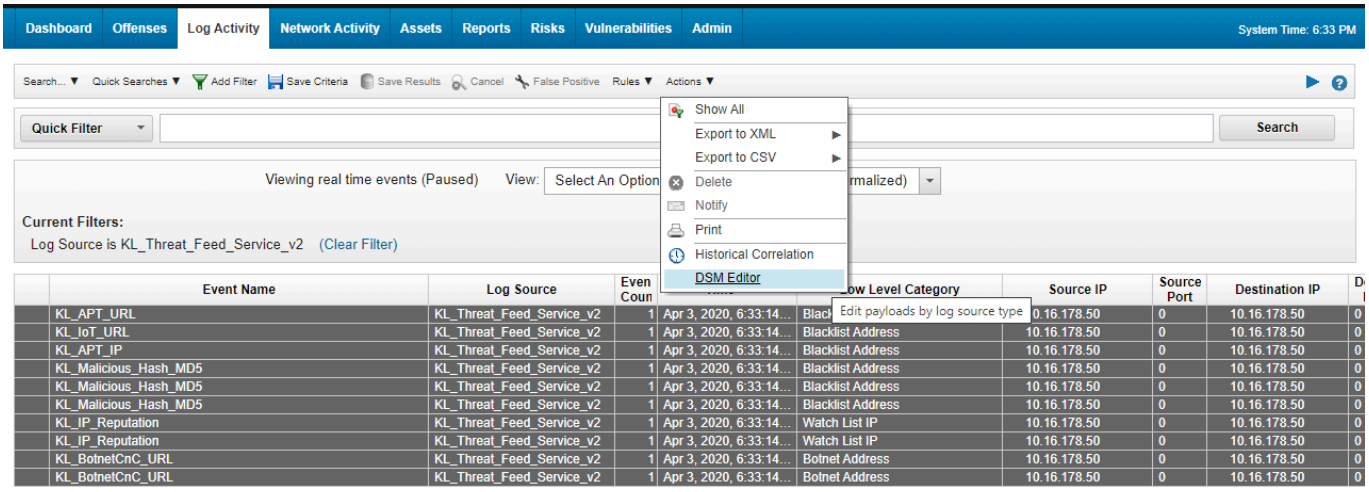


Добавление фильтра

3. Нажмите на кнопку **Add Filter**.

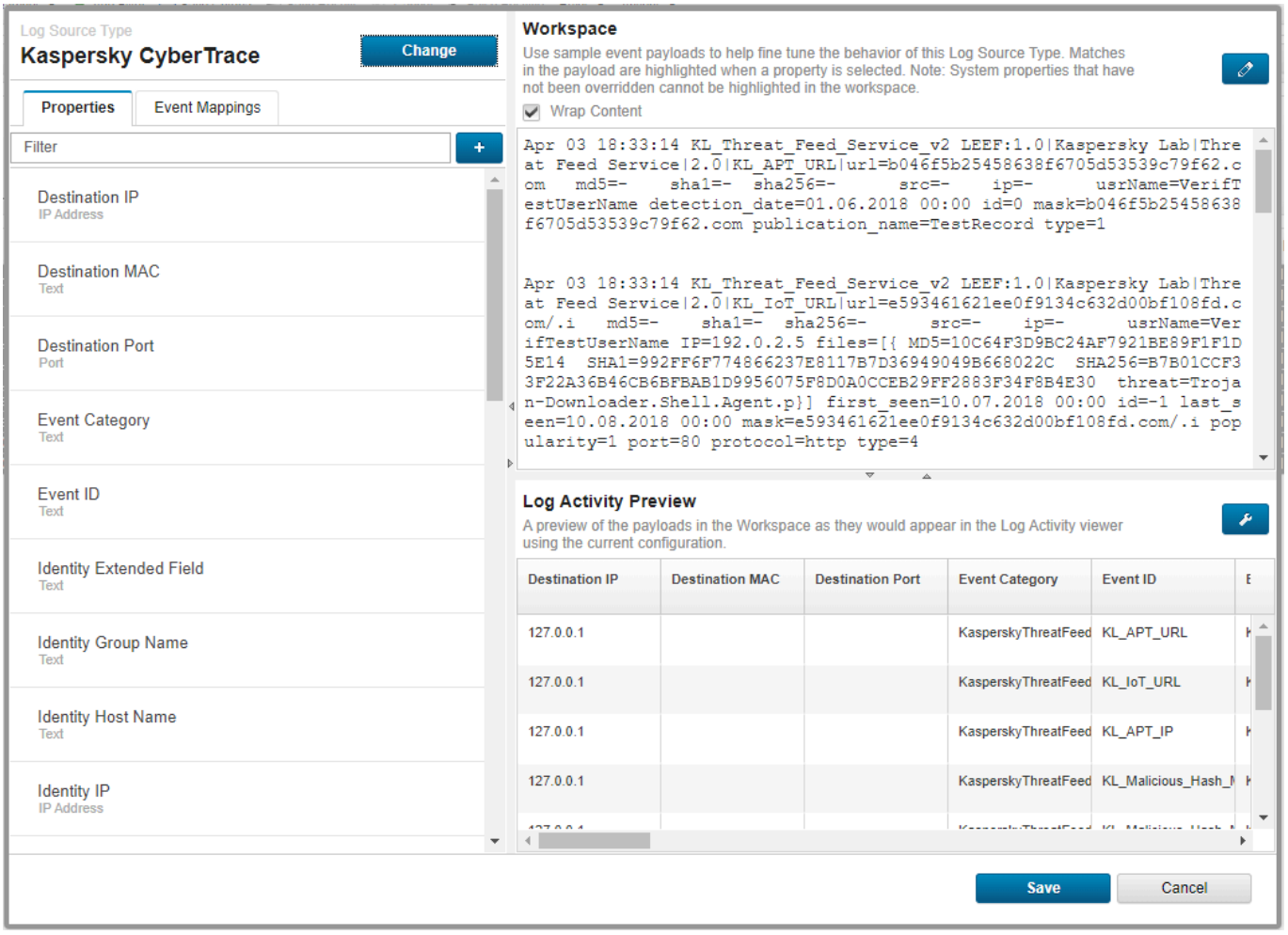
4. Выполните проверку работоспособности, затем остановите поток событий, нажав кнопку **Pause** (⏸) в правом верхнем углу окна.

5. Выберите несколько записей, удерживая клавишу **`Ctrl`** (или **`Shift`**), затем выберите **Actions** → **DSM editor**.



Окно **Log Activity**

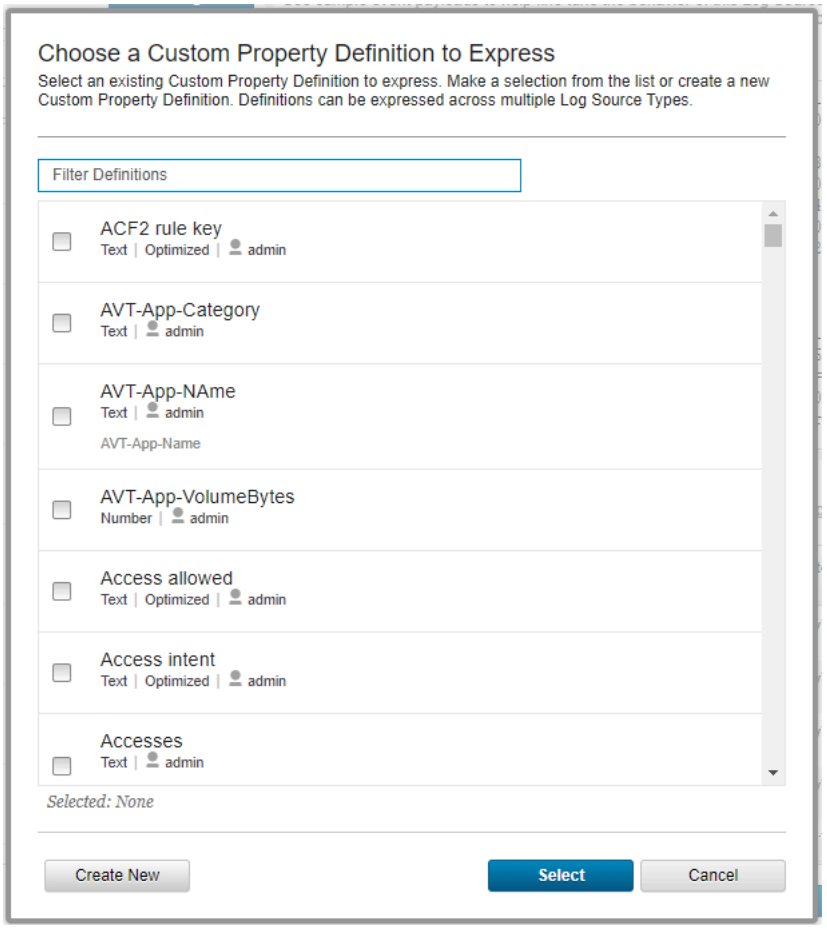
Откроется окно **DSM Editor**.



Окно DSM Editor

6. В окне **DSM Editor** нажмите кнопку **+** рядом с полем ввода **Filters**.

Откроется форма **Choose a Custom Property Definition to Express**.



Выбор пользовательского свойства

7. Нажмите на кнопку **Create new**.

   Откроется форма **Create a new Custom Property Definition**.

8. Заполните эту форму:

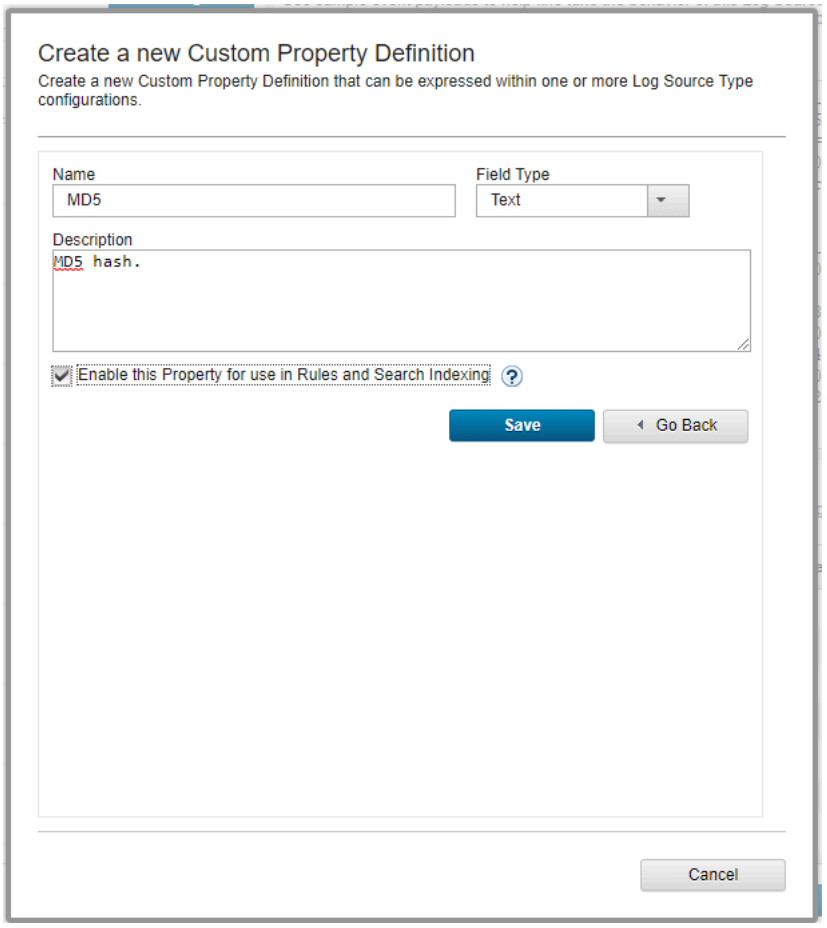
   a. В поле **Name** укажите `MD5`.

   b. В раскрывающемся списке **Field Type** выберите `Text`.

   c. В поле **Description** введите описание свойства.

d. Установите флажок **Enable this Property for Use in Rules and Search Indexing**.

e. Нажмите на кнопку **Save**.



Создание нового определения пользовательского свойства

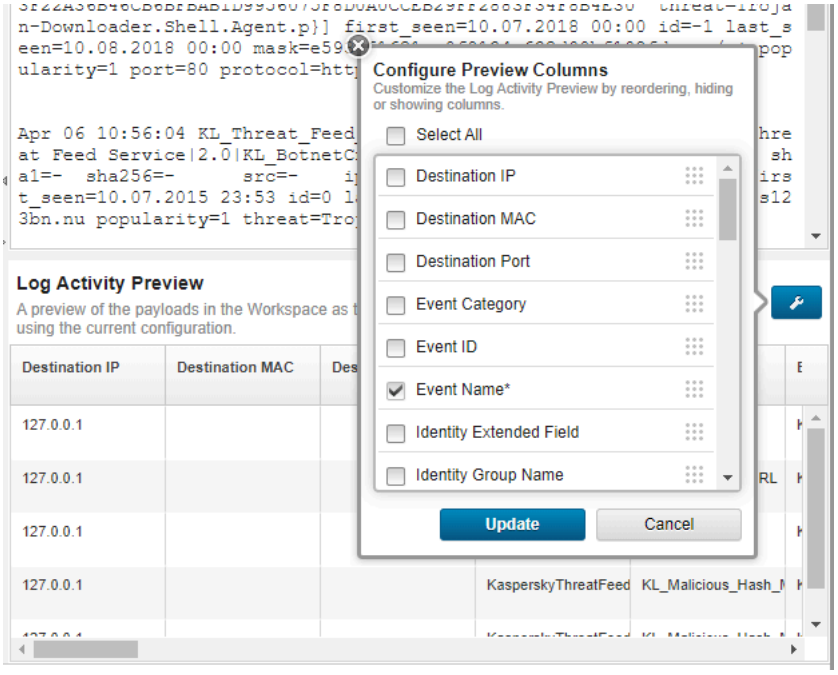
9. Аналогичным образом добавьте свойства `SHA1` и `SHA256`.

10. В окне **Choose a Custom Property Definition to Express** выберите созданные свойства, добавьте URL и IP-адрес источника (Source IP), затем нажмите кнопку **Select**.

11. В разделе **Log Activity Preview** нажмите **Configure** и выберите следующие свойства:

    - `Event Name`
    - `IP (custom)`
    - `MD5 (custom)`
    - `SHA1 (custom)`
    - `SHA256 (custom)`
    - `Source IP`
    - `URL (custom)`
    - `Username`

Нажмите **Update**.



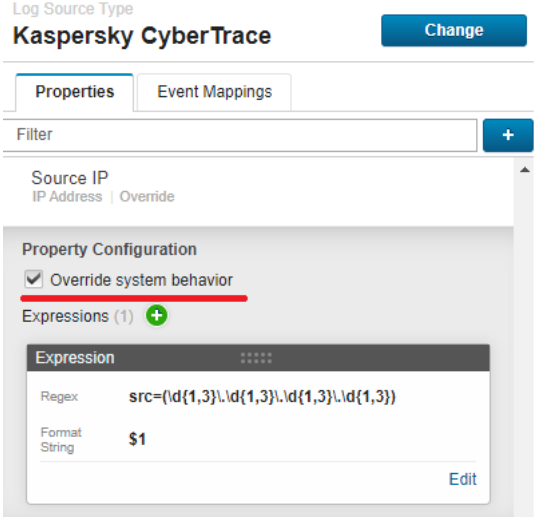
Настройка столбцов предварительного просмотра

12. На вкладке **Properties** настройте регулярные выражения, как описано в таблице ниже:

Пользовательское свойство	Регулярное выражение
MD5	`md5=([\da-fA-F]{32})`
SHA1	`sha1=([\da-fA-F]{40})`
SHA256	`sha256=([\da-fA-F]{64})`
URL	`url=([-a-zA-Z0-9()@:%_\+.~#?&\/\/=]{2,})`
Source IP	`src=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})`

Если необходимо, введите `1` в поле **Capture Group**.

13. Для свойства **Source IP** установите флажок **Override system behavior**.



Настройка IP-адреса источника

При изменении формата исходящих событий обнаружения киберугроз в Kaspersky CyberTrace может потребоваться внесение соответствующих изменений в указанные выше регулярные выражения.

Если все вышеперечисленные настройки заданы правильно, настроенные **пользовательские свойства** отображаются в разделе **Log Activity Preview**.

14. Нажмите на кнопку **Save** и закройте окно.

15. На вкладке **Log Activity** выполните новую проверку работоспособности.

    После этого при открытии события, полученного от `KL_Threat_Feed_Service_v2`, будут отображаться настроенные пользовательские свойства.

Event Information

Event Name	KL_IP_Reputation						
Low Level Category	Watch List IP						
Event Description	IP match found by Kaspersky Threat Feed Service						
Magnitude	(4)	Relevance	3	Severity	4	Credibility	5
Username	VerifTestUserName						
Start Time	Apr 6, 2020, 10:56:14 AM	Storage Time	Apr 6, 2020, 10:56:14 AM	Log Source Time	Apr 6, 2020, 10:56:04 AM		
IP (custom)	192.0.2.0						
MD5 (custom)	N/A						
SHA1 (custom)	N/A						
SHA256 (custom)	N/A						
URL (custom)	N/A						
Domain	Default Domain						

Source and Destination Information

Source IP	[redacted]	Destination IP	[redacted]
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
IPv6 Source	0:0:0:0:0:0:0:0	IPv6 Destination	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Информация о событии

Шаг 6. Создание поискового фильтра для событий Kaspersky CyberTrace

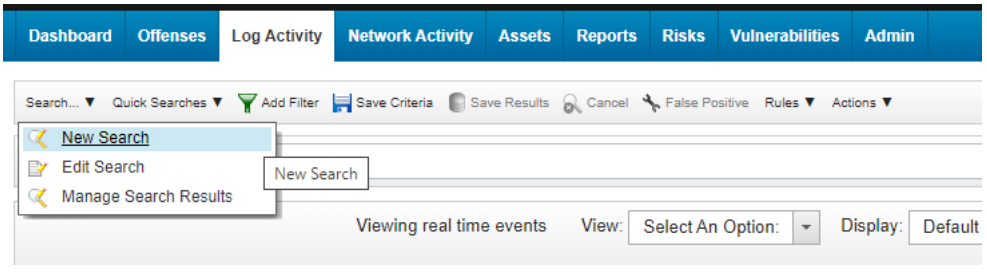
В этом разделе описывается порядок создания поиска событий.

Чтобы создать поиск событий, выполните следующие действия.

1. Остановите поток событий, нажав кнопку **Pause** (⏸) в правом верхнем углу окна.

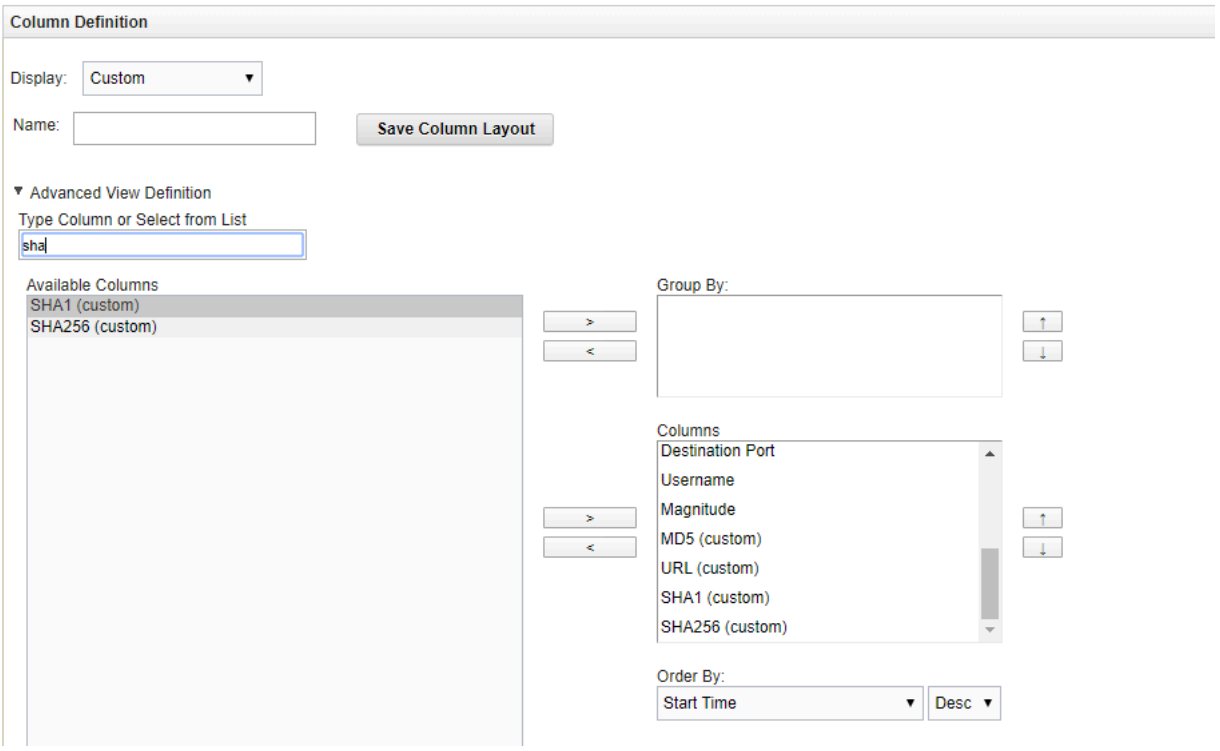
2. В QRadar Console перейдите на вкладку **Log Activity**.

3. Выберите **Search** → **New Search**.



Новый поиск

4. В форме **Column Definition** добавьте `MD5 (custom)`, `SHA1 (custom)`, `SHA256 (custom)`, `URL (custom)`, `IP (custom)` из списка **Available Columns** в список **Columns**.



Определение столбцов

5. Прокрутите страницу вниз и в форме **Search Parameters** задайте `KL_Threat_Feed_Service_v2` в качестве источника журналов:

   a. В раскрывающемся списке **Parameter** выберите `Log Source [Indexed]`.

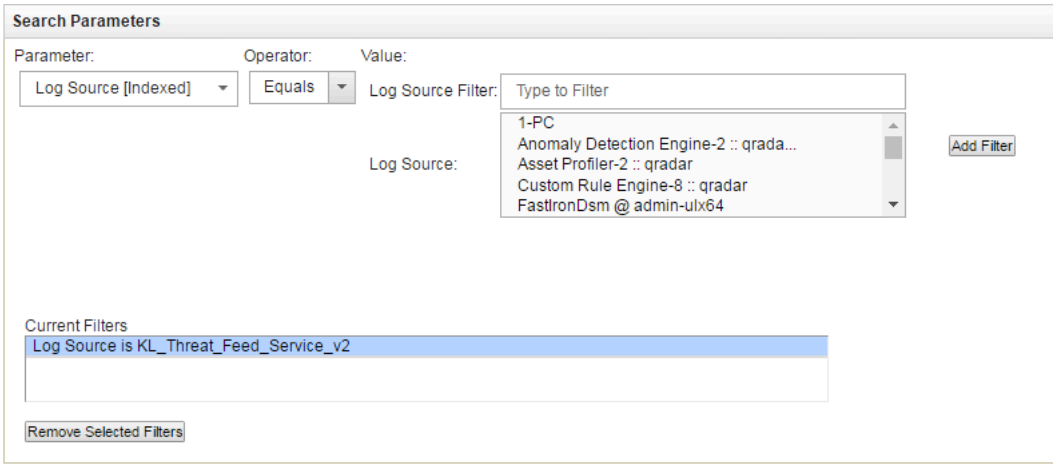
   b. В раскрывающемся списке **Operator** выберите `Equals`.

   c. В списке **Log Source** выберите `KL_Threat_Feed_Service_v2`.

   Вариант выбора `KL_Threat_Feed_Service_v2` соответствует имени источника журналов, заданному в элементе `OutputSettings` > `EventFormat` и в элементе `OutputSettings` > `AlertFormat` конфигурационного файла Kaspersky CyberTrace Service (их также можно задать с помощью веб-интерфейса Kaspersky CyberTrace).

   d. Нажмите на кнопку **Add Filter**.

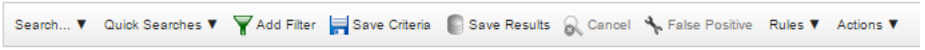
   В список **Current Filters** будет добавлена строка `Log Source is KL_Threat_Feed_Service_v2`.



Настройка источника журнала

6. Нажмите на кнопку **Search**, чтобы отобразить результат поиска.

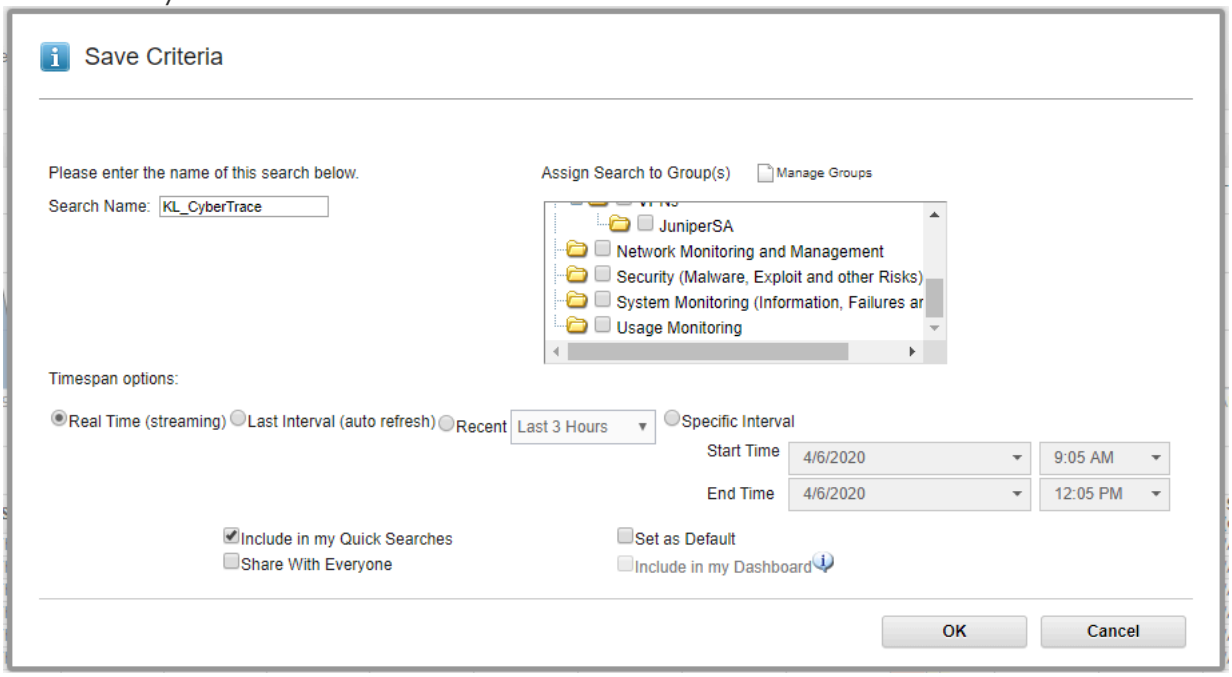
7. Нажмите на кнопку **Save Criteria**.



Кнопка **Save Criteria**

8. В форме **Save Criteria** введите имя поиска в поле ввода **Search Name**, установите флажок **Include in my Quick Searches**, затем укажите анализируемый интервал для созданного поиска (например, **Real Time**).

9. Нажмите на кнопку **OK**.



Сохранение критериев

Шаг 7 (необязательный). Отображение событий на информационной панели

На информационной панели QRadar наглядно отображаются результаты обнаружения киберугроз. Например, на диаграмме отображается соотношение количества событий разного типа.

Требуется QRadar 7.2.6 Patch 3 или более поздняя версия. Использование более ранней версии может привести к неверным результатам.

Для добавления диаграммы, отображающей результаты обнаружения киберугроз Kaspersky CyberTrace Service в визуальном формате, необходимо выполнить три процедуры:

1. Создание поиска событий.

2. Добавление диаграммы на информационную панель.

3. Настройте добавленную диаграмму.

Создание поиска событий

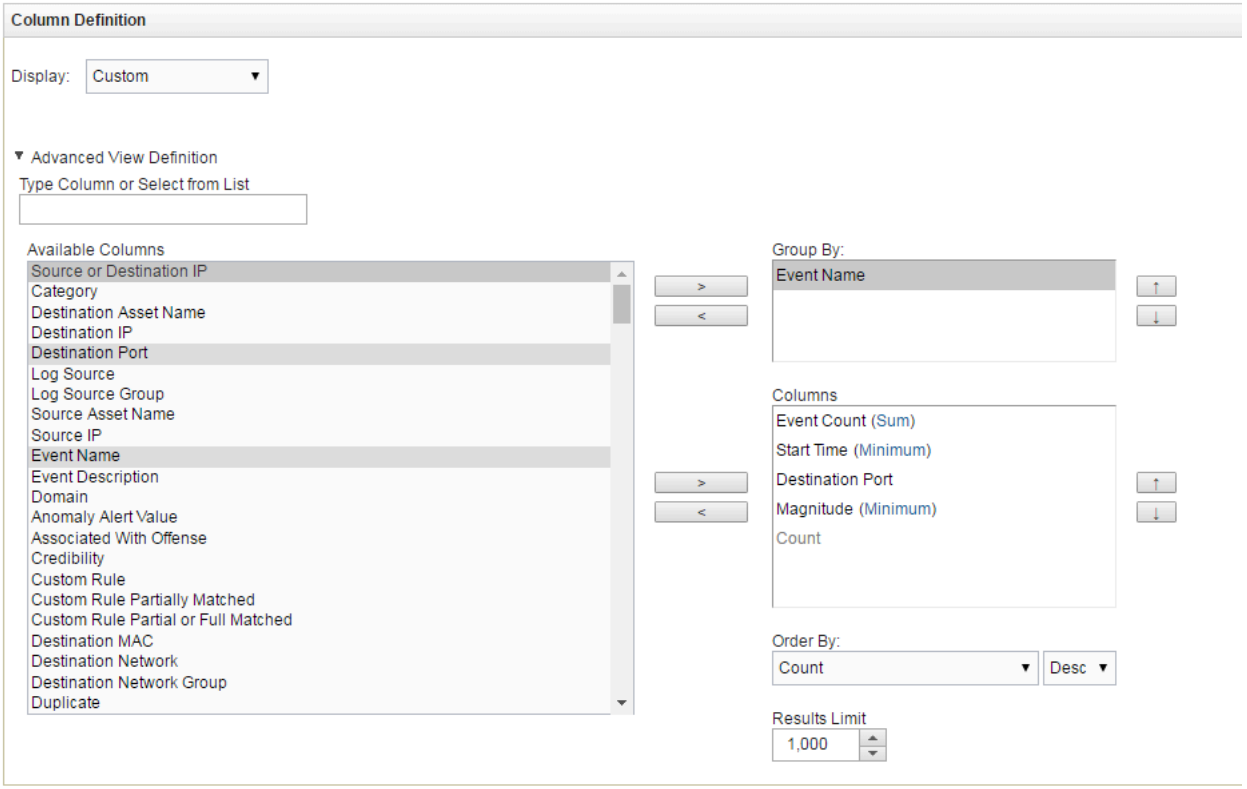
Далее описывается порядок создания поиска событий.

Чтобы создать поиск событий, выполните следующие действия:

1. В QRadar Console перейдите на вкладку **Log Activity**.

2. Выберите **Search** → **New Search**.

3. В форме **Column Definition** удалите `Event Name` из списка **Available Columns** и добавьте `Event Name` в список **Group By**.



Определение столбцов

4. Прокрутите страницу вниз и в форме **Search Parameters** задайте `KL_Threat_Feed_Service_v2` в качестве источника журналов:

   a. В раскрывающемся списке **Parameter** выберите `Log Source [Indexed]`.

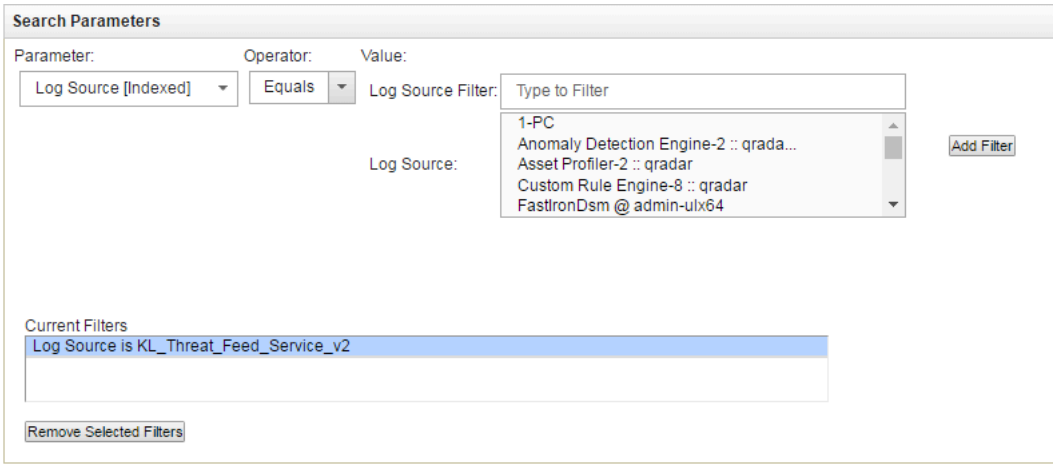
   b. В раскрывающемся списке **Operator** выберите `Equals`.

   c. В списке **Log Source** выберите `KL_Threat_Feed_Service_v2`.

   Вариант `KL_Threat_Feed_Service_v2` соответствует имени источника журналов, который задан в параметрах формата событий обнаруженных киберугроз и формата оповещений о событиях на вкладке Форматы событий в веб-интерфейсе Kaspersky CyberTrace.

d. Нажмите на кнопку **Add Filter**.

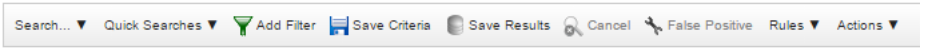
В список **Current Filters** будет добавлена строка `Log Source is KL_Threat_Feed_Service_v2`.



Настройка источника журнала

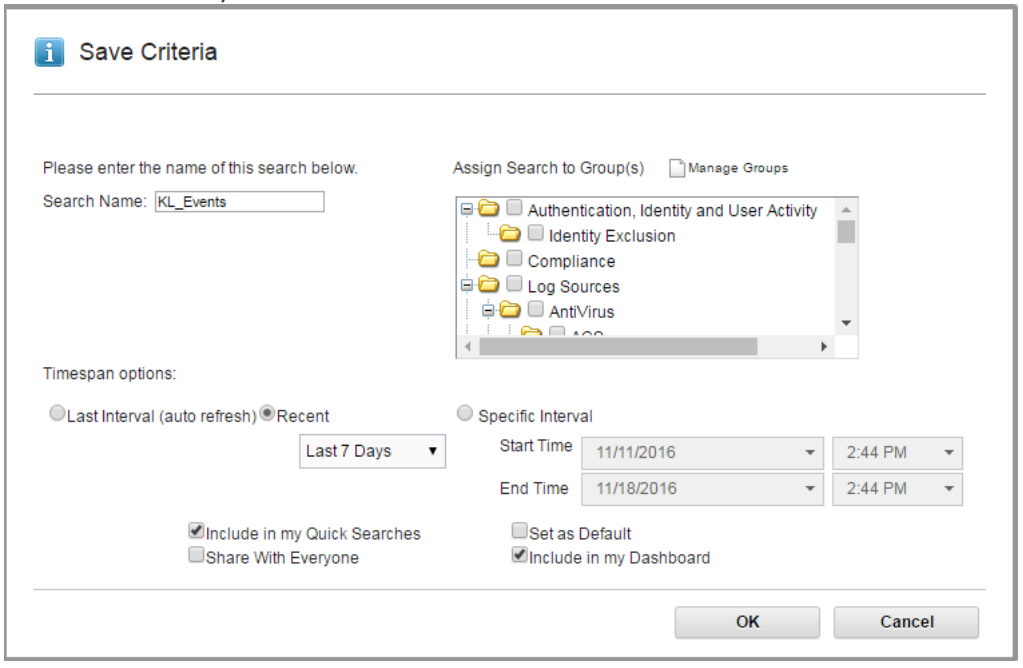
5. Нажмите на кнопку **Filter** или **Save**, чтобы отобразился результат поиска.

6. Нажмите на кнопку **Save Criteria**.



Кнопка **Save Criteria**

7. В форме **Save Criteria** установите флажок **Include in my Dashboard**, введите имя поиска в поле ввода **Search Name** и нажмите кнопку **OK**.



Сохранение критериев

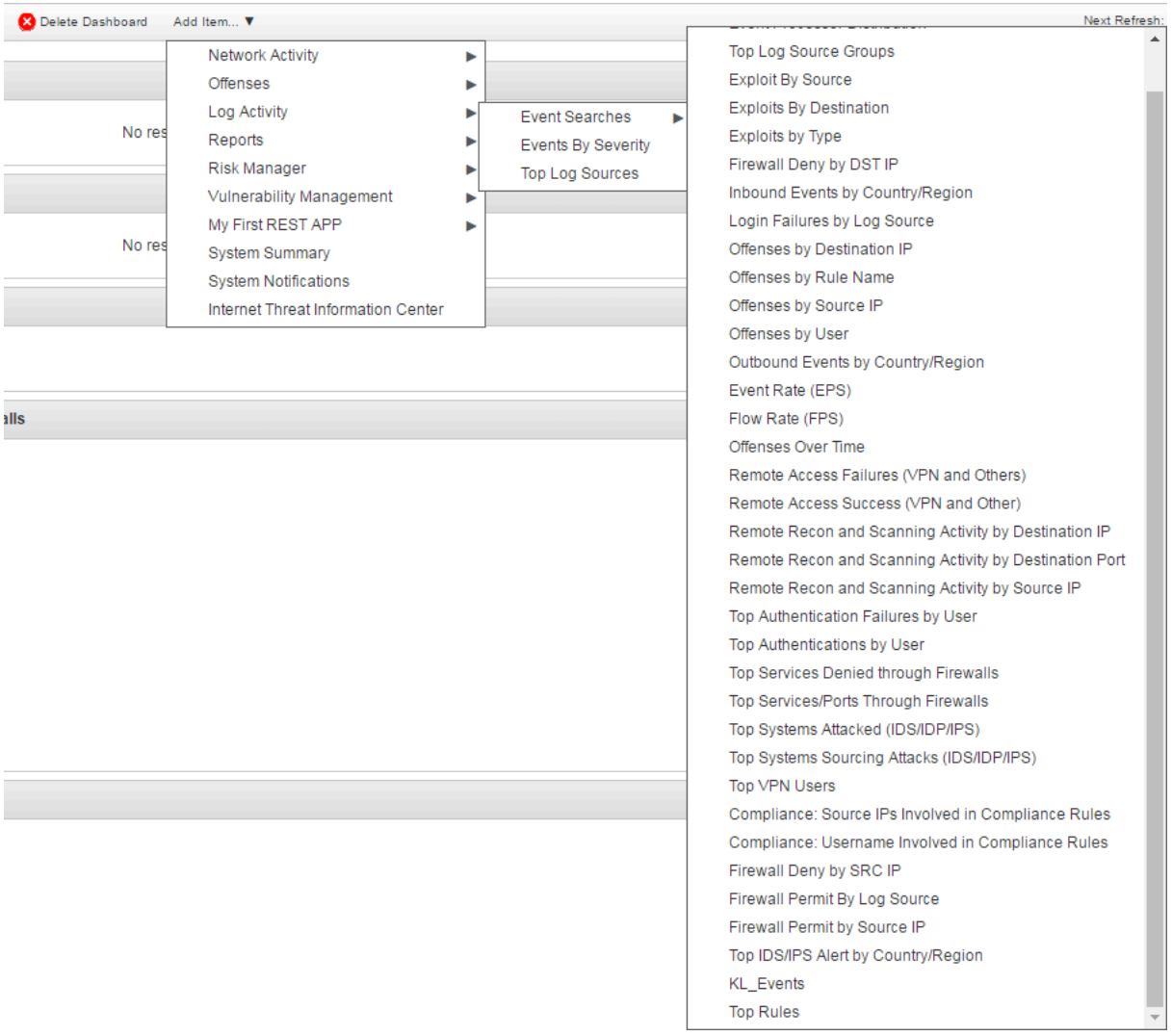
Добавление диаграммы на информационную панель

Следующая процедура описывает порядок добавления диаграммы на информационную панель.

Чтобы добавить диаграмму на информационную панель:

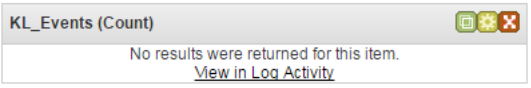
1. В QRadar Console выберите вкладку **Dashboard**.
2. Выберите **Add Item** → **Log Activity** → **Event Searches** → **KL_Events**.

   Здесь `KL_Events` — это имя заданного поиска.



Добавление элемента на информационную панель

   На информационной панели появится диаграмма.



Новая диаграмма

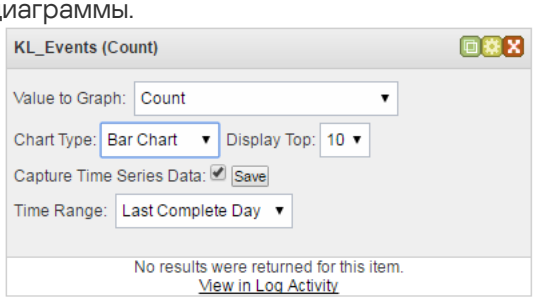
Настройка добавленной диаграммы

Следующая процедура описывает порядок настройки диаграммы, добавленной на информационную панель.

Чтобы настроить добавленную диаграмму, выполните следующие действия:

1. Нажмите на кнопку **Settings** ( ) в правом верхнем углу диаграммы.

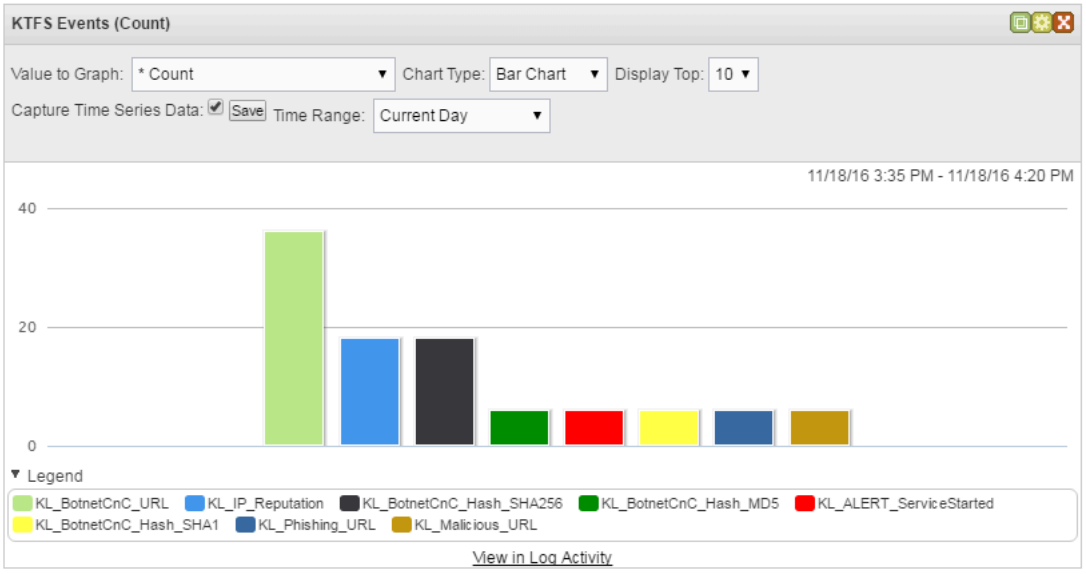
2. Задайте требуемые настройки диаграммы.



Настройки диаграммы

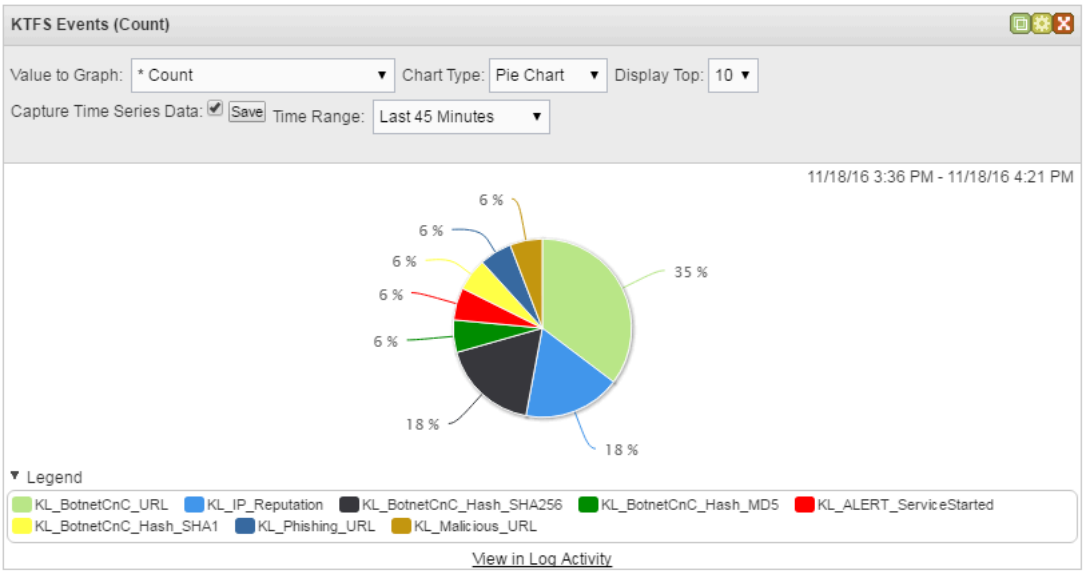
Если установлен флажок **Capture Time Series Data**, на диаграмме будут отображаться все входящие данные, полученные после установки этого флажка; при этом выбор в раскрывающемся списке **Time Range** игнорируется. Если снять флажок **Capture Time Series Data**, будет отображаться только информация, полученная в течение временного интервала, выбранного в раскрывающемся списке **Time Range**.

После поступления событий они отображаются на диаграмме.



Гистограмма

В раскрывающемся списке **Chart Type** можно выбрать тип диаграммы, который будет использоваться для отображения данных.



Круговая диаграмма

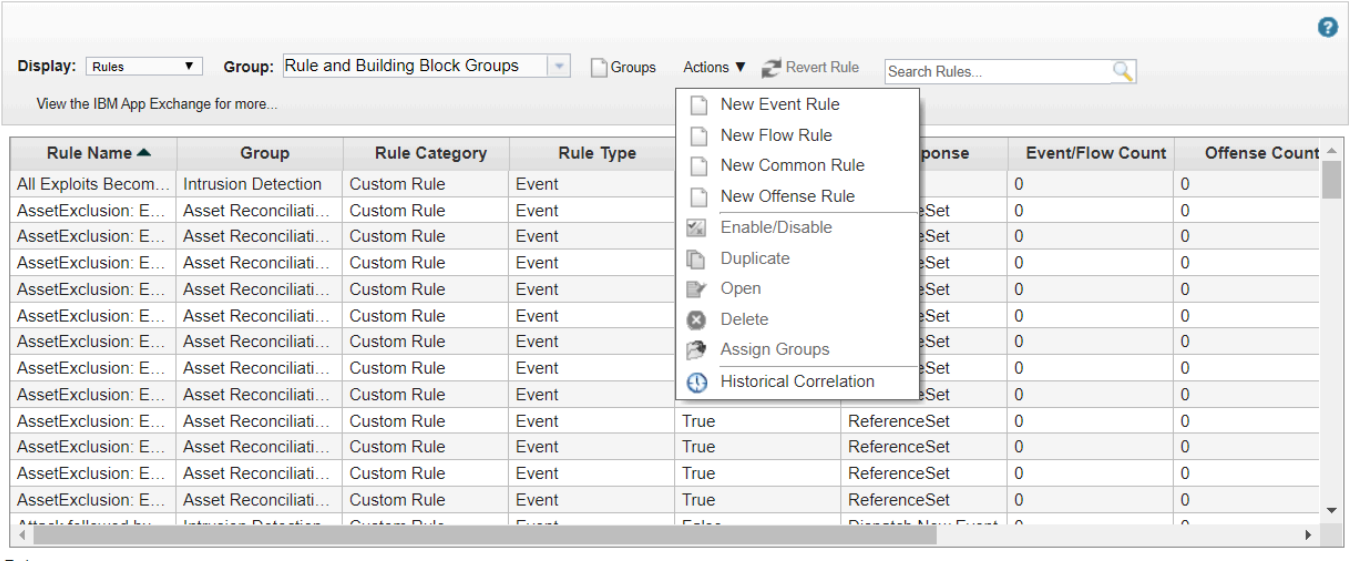
Информация о диаграммах, основанных на результатах поиска, также приведена в справке QRadar (раздел «Dashboard management → Adding search-based dashboard items to the Add Items list»).

Шаг 8 (необязательный). Создание уведомлений о входящих служебных событиях

Для создания уведомлений о проблемах с Kaspersky CyberTrace можно настроить правила оповещений.

Чтобы создать уведомления о служебных событиях из Kaspersky CyberTrace в QRadar, выполните следующие действия:

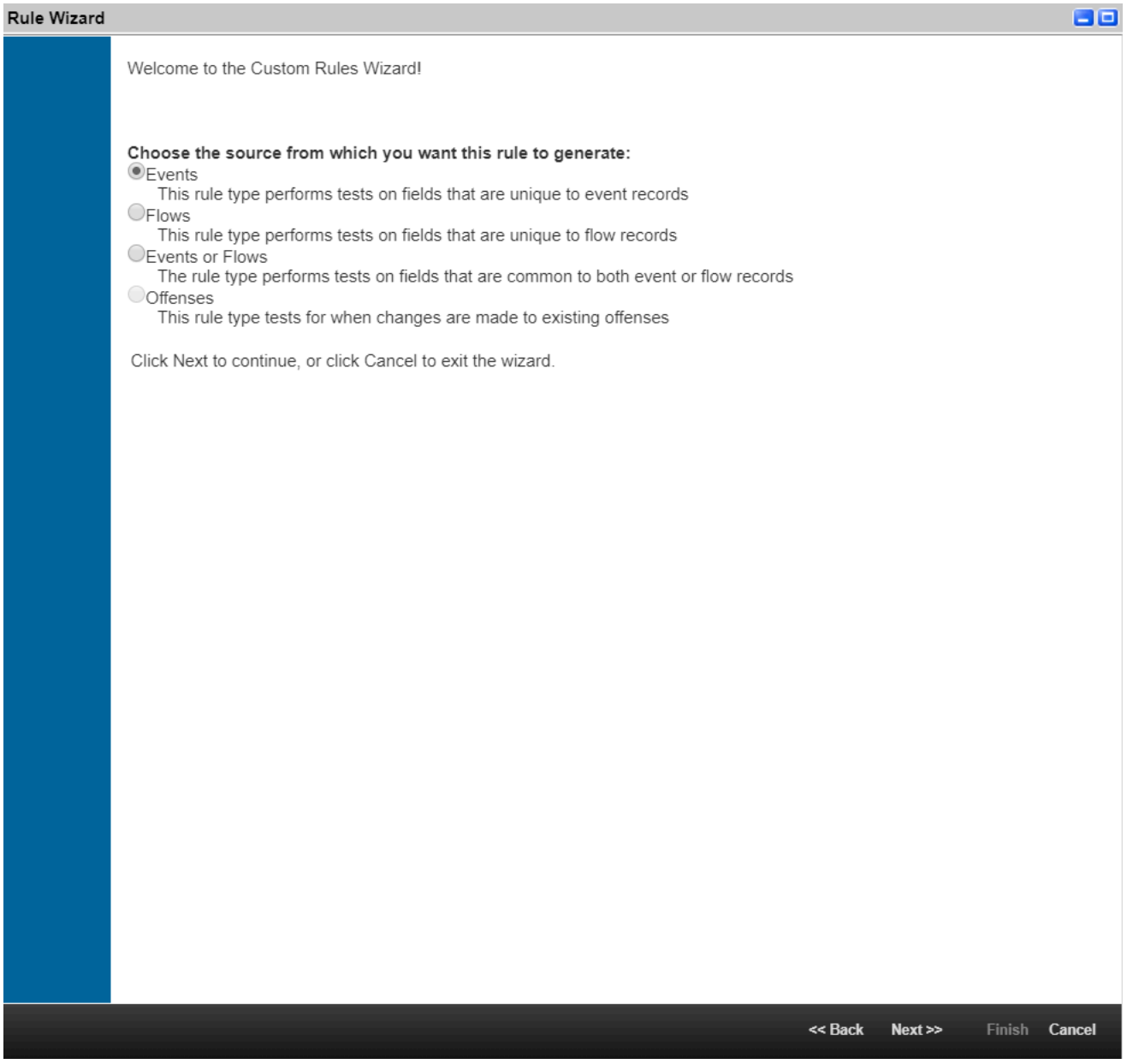
1. Запустите QRadar Console.
2. Выберите любую из вкладок: **Offenses**, **Log Activity** или **Network Activity**, затем выберите **Rules**.
3. В раскрывающемся списке **Actions** выберите **New Event Rule**.



Страница **Rules**

Откроется страница **Rule Wizard**.

4. На странице **Rule Wizard** нажмите кнопку **Next**, чтобы выбрать источник, из которого требуется создать правило.



Окно **Rules Wizard**

5. Выберите **Events**, затем нажмите **Next**.

6. На странице **Rule Test Stack Editor** выполните следующие действия:

   - Добавьте следующие тестовые условия для нового правила:

     - `when the event(s) were detected by one or more of these log sources`

     - `when the event matches this search filter`

   - Для каждого указанного условия задайте логический оператор `and`.

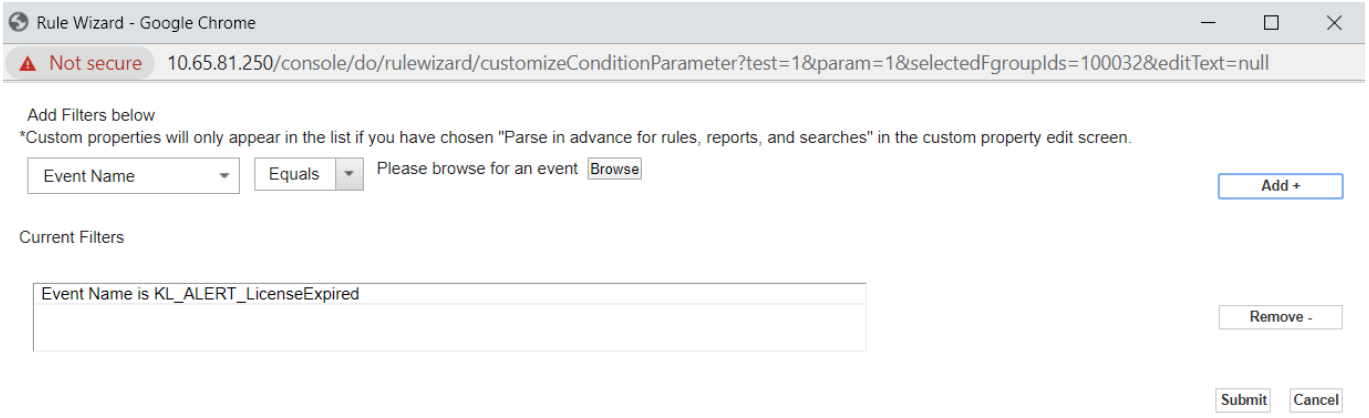
   - Для условия `when the event(s) were detected by one or more of these log sources` укажите значение **Log Source** `KL_Threat_Feed_Service_v2`. Если этот источник событий отсутствует, добавьте Kaspersky CyberTrace Service в качестве источника журналов.

- Для условия `when the event matches this search filter` задайте фильтр для сравнения имени события (**Event Name**) со значением имени источника событий, для этого выполните следующие действия:

  a. В списке полей событий выберите **Event Name**.

  b. В списке условий выберите **Equals**.

  c. Нажмите кнопку **Browse** и выберите имя служебного события, для которого создается правило.

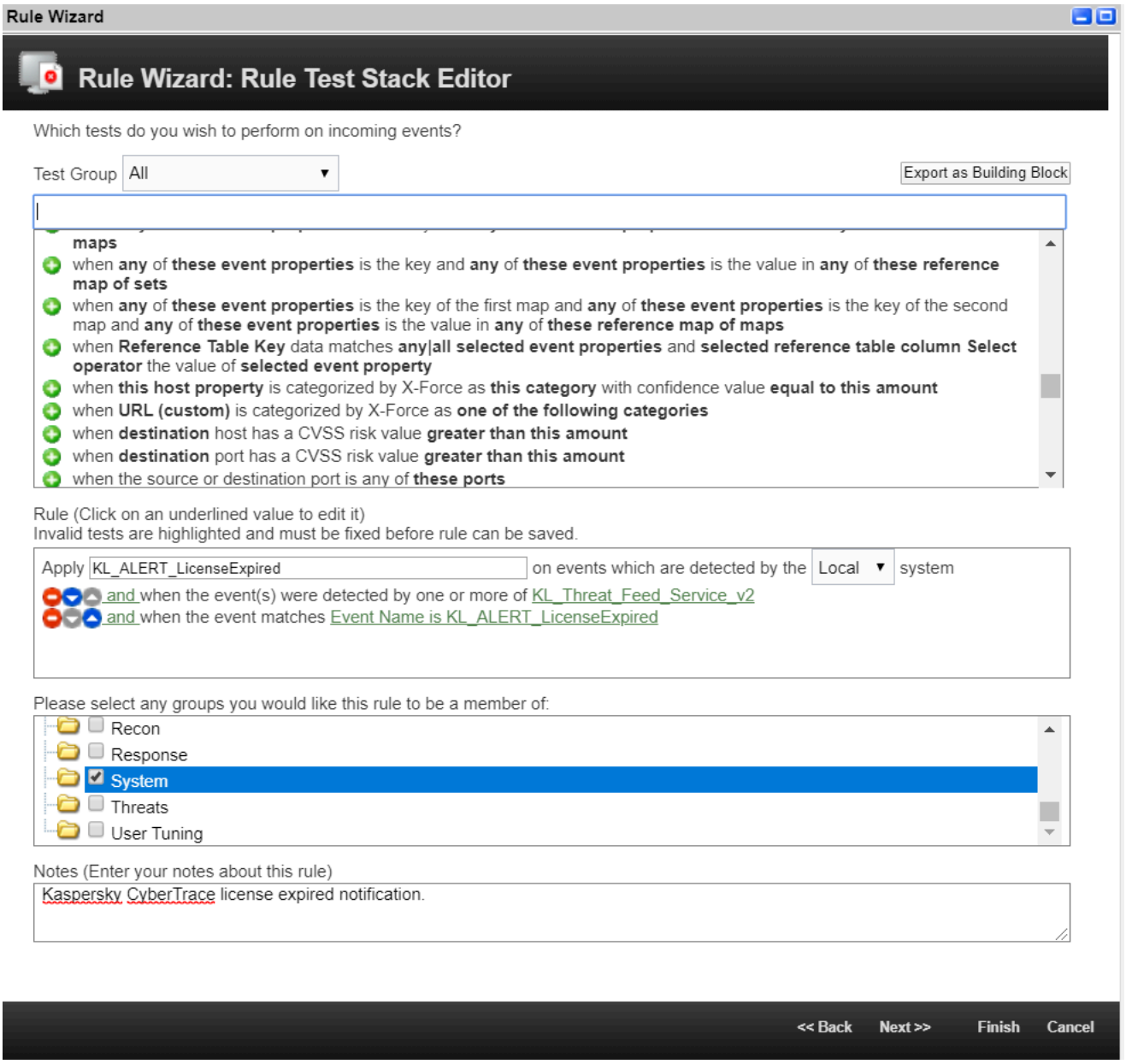


Добавление фильтров

a. Нажмите на кнопку **Add+**, затем **Submit**.

> Если необходимое событие отсутствует, добавьте его в список идентификаторов QRadar Identifier (QID).

- Введите имя правила и выберите способ применения этого правила к входящим событиям (**Local** или **Global**). Дополнительная информация о правилах *Local* и *Global* приведена в документации IBM.
- Выберите группу, необходимую для правила.
- Добавьте описание правила.

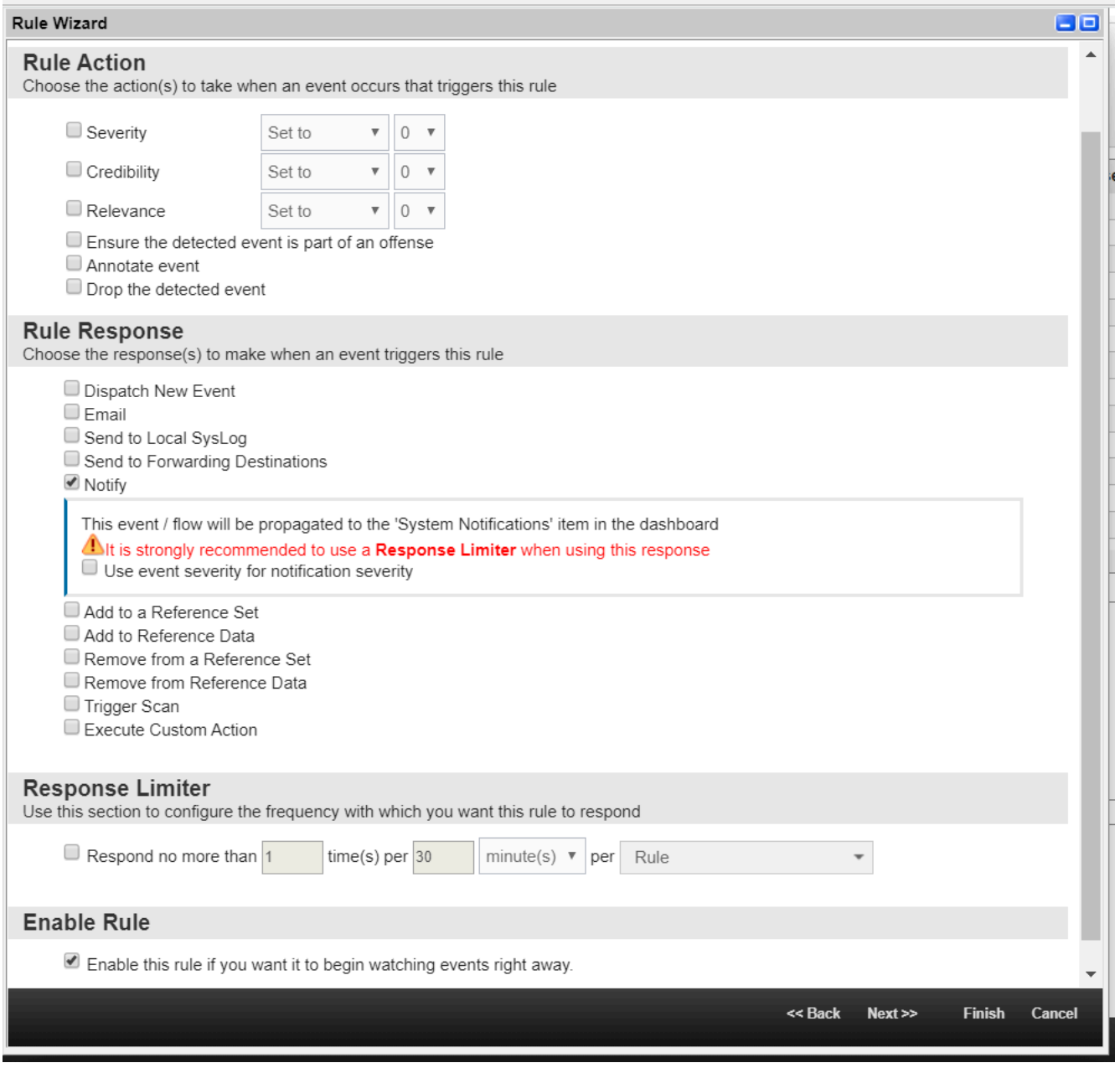


Окно Rule Editor

- Нажмите на кнопку **Next**.

7. На странице **Rule Response** выполните следующие действия:

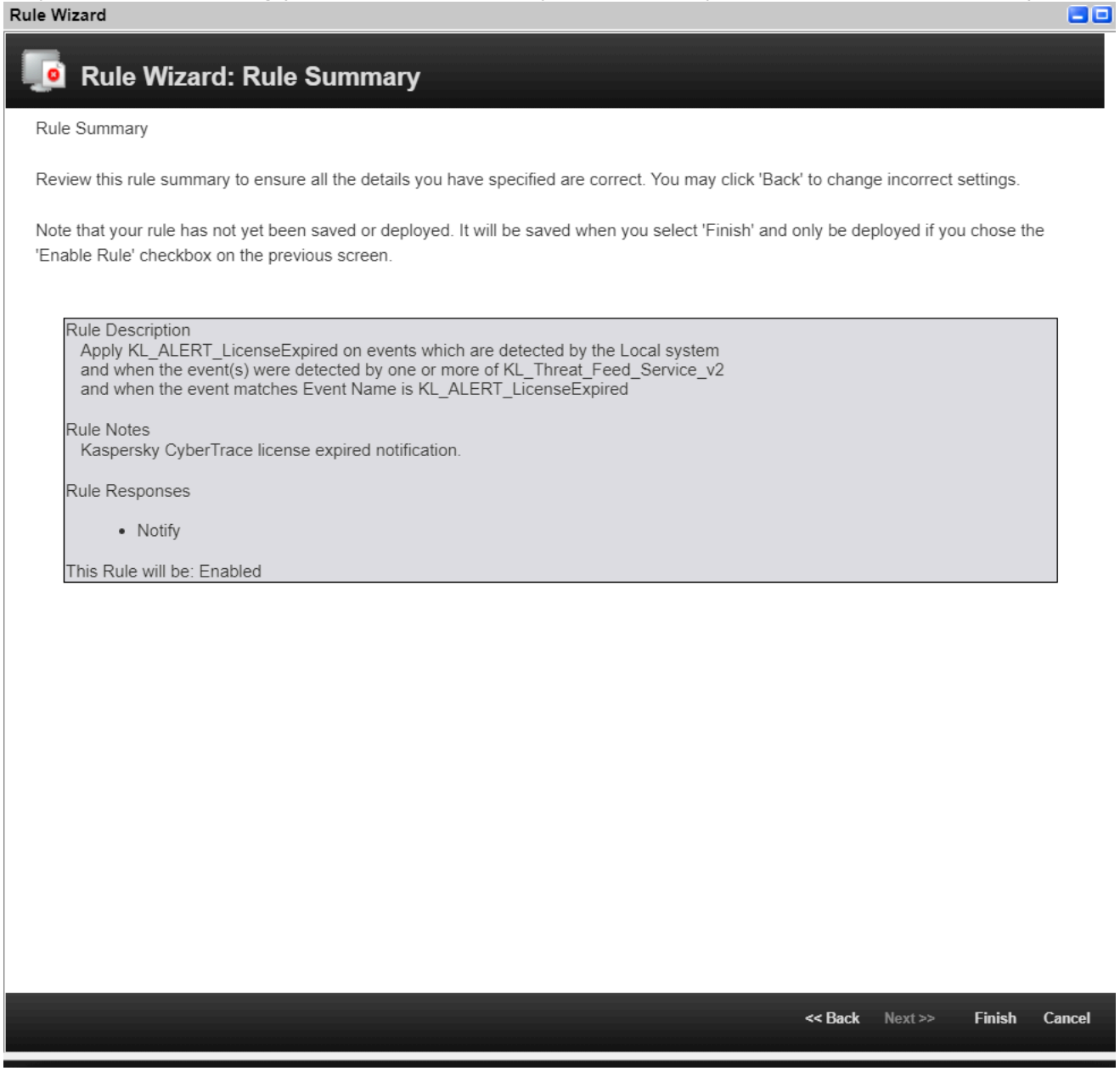
- Выберите **Notify**.
- При необходимости задайте ограничение на срабатывание правила в разделе **Response Limiter**.
- Проверьте раздел **Enable Rule**.



Страница **Rule Editor**

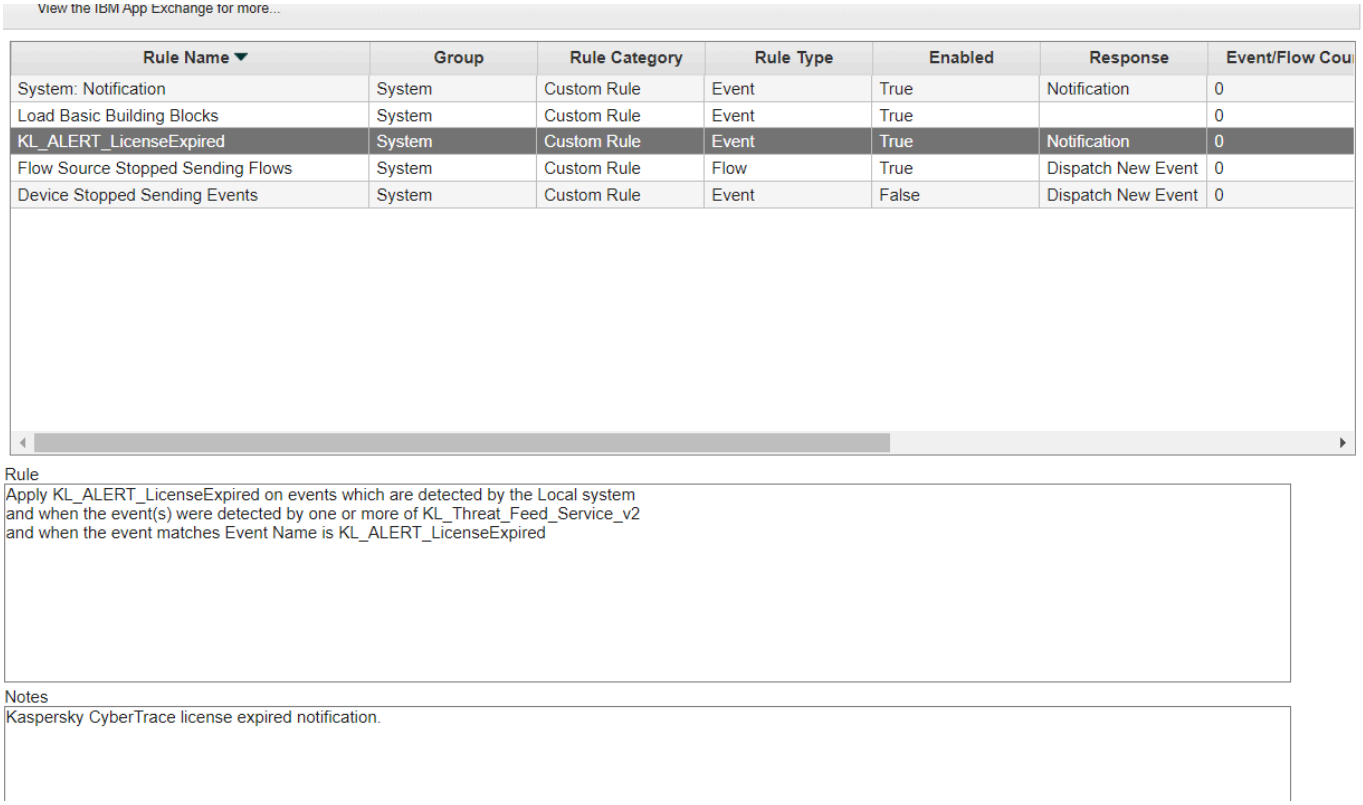
- Нажмите на кнопку **Next**.

8. На странице **Rule Summary** убедитесь, что все настройки заданы правильно, и нажмите на кнопку **Finish**.



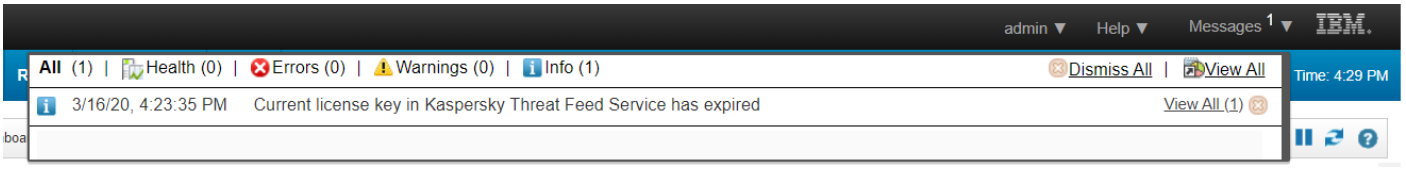
Страница **Rule Summary**

Правило добавляется в список **Rules**.



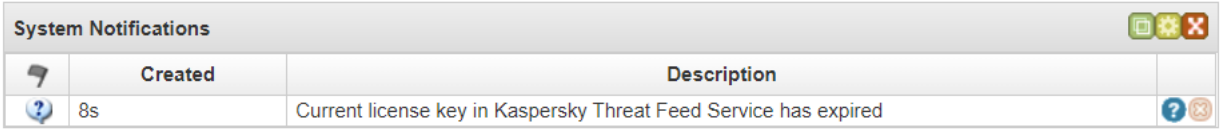
Список **Rules**

Добавленное правило генерирует уведомление о входящем служебном событии. Для просмотра этих уведомлений можно нажать на раскрывающийся список **Messages**. Кроме того, уведомления отображаются в QRadar Console в виде всплывающих уведомлений.



Раскрывающийся список **Messages**

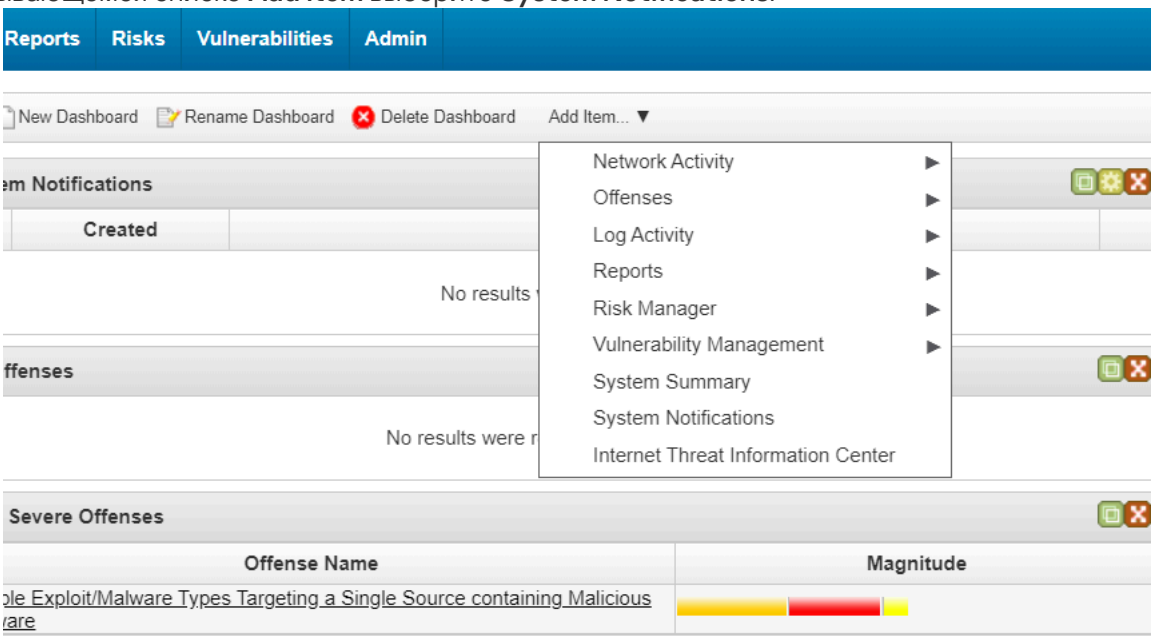
Настроить отображение уведомлений можно на вкладке **Dashboard**.



Системные уведомления на вкладке **Dashboard**

*Чтобы настроить отображение уведомлений на вкладке **Dashboard**, выполните следующие действия:*

1. Выберите вкладку **Dashboard**.
2. В раскрывающемся списке **Add Item** выберите **System Notifications**.



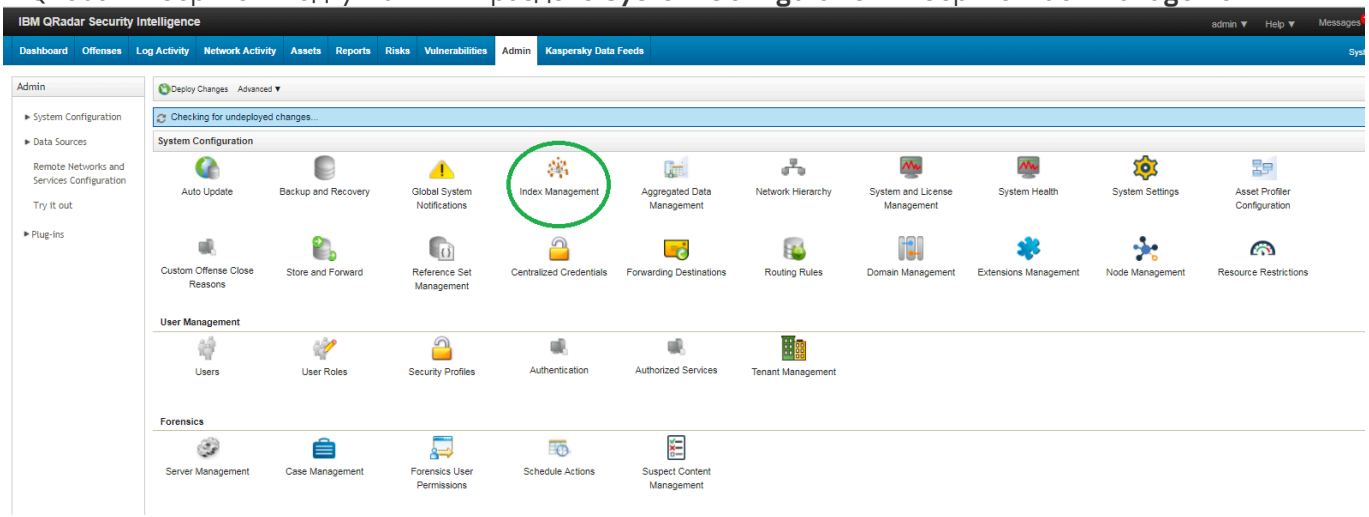
Добавление системных уведомлений на вкладку **Dashboard**

Шаг 9 (необязательный). Включение индексов добавленных свойств пользовательского события

Рекомендуется включить индексы добавленных пользовательских свойств событий. Это повысит производительность приложения Kaspersky CyberTrace App for QRadar.

Чтобы включить индексы добавленных пользовательских свойств событий, выполните следующие действия:

1. В QRadar выберите вкладку **Admin** и в разделе **System Configuration** выберите **Index Management**.



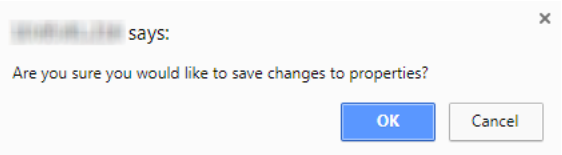
Вкладка **Admin** в QRadar Console (инструменты настройки системы)

Откроется окно **Index Management**.

2. Дополнительно можно указать фильтр для поиска добавленных свойств.
3. Выберите одну или несколько строк таблицы и нажмите на кнопку **Enable Index**.

4. Нажмите на кнопку **Save**.

   Появится окно сообщения с запросом сохранения внесенных изменений.



Сохранение изменений индексов

5. Нажмите на кнопку **OK**, чтобы сохранить изменения свойств.

Альтернативная интеграция (QRadar)

В этой главе описывается порядок интеграции Kaspersky CyberTrace с QRadar.

Это дополнительный сценарий для случая, когда невозможно получать обновления QRadar.

Интеграция с QRadar в случае, если QRadar не может получать обновления

Если получать последние обновления QRadar невозможно, выполните настройку в последовательности, описанной ниже.

Чтобы использовать QRadar вместе с Kaspersky CyberTrace Service, если обновление QRadar невозможно:

1. Импортируйте новые идентификаторы QRadar в QRadar.
2. Добавьте Kaspersky CyberTrace Service в качестве источника журналов для QRadar.
3. Сопоставьте события Kaspersky CyberTrace Service с идентификаторами QRadar.
4. Укажите тип источника журналов.
5. Выполните проверку работоспособности.
6. (Необязательно) Выполните все шаги из следующих инструкций: настройте в QRadar отображение пользовательских полей событий.
7. (Необязательно) Выполните все шаги из следующих инструкций: настройте в QRadar отображение событий на информационной панели.

Импорт QID в QRadar

QRadar должен правильно обрабатывать входящие события от Kaspersky CyberTrace Service. Для этого необходимо добавить в QRadar список допустимых событий (список идентификаторов QRadar — QID). В Kaspersky CyberTrace Service категории событий определяются в конфигурационном файле в элементе `Feeds > Feed > Field`, в атрибуте `category`.

В состав комплекта поставки Kaspersky CyberTrace входит файл sample_qid.txt, содержащий необходимые события от Kaspersky CyberTrace Service. Описания этих событий изменять не следует, вместо этого добавьте в файл собственные события.

Рекомендуется присваивать имена категориям событий в соответствии с форматом «KL_<feed>_<object_type>», где:

- <feed> — имя потока данных об угрозах, обнаруживающего событие (например, PhishingUrl.
- <object_type> — поле, по которому обнаруживается событие (например, URL, Hash_MD5, Hash_SHA1, Hash_SHA256).

Чтобы импортировать список QID в QRadar, выполните следующие действия:

1. При необходимости (например, если это рекомендует сделать ваш персональный технический менеджер) отредактируйте файл %service_dir%/integration/qradar/sample_qid.txt, добавив в него все категории событий, содержащиеся в конфигурационном файле.

   Каждая категория событий должна быть описана на отдельной строке в следующем формате:

   ,<event>,<descr>,<sev>,<cat_id>

   где:

   - <event> — имя входящего события.
   - <descr> — описание события.
   - <sev> — уровень важности события.
   - <cat_id> — низкоуровневый идентификатор события QRadar.

     Полный список идентификаторов событий QRadar вывести с помощью следующей команды:

     /opt/qradar/bin/qidmap_cli.sh -l

     Рекомендуется выбирать значения <sev> и <cat_id> в соответствии с документацией QRadar.

   Например:

   ,KL_Malicious_URL,Malicious URL is detected by Kaspersky Threat Feed Service,8,7058

2. Загрузите файл %service_dir%/integration/qradar/sample_qid.txt на сервер, на котором установлен QRadar.
3. Вызовите команду:

   /opt/qradar/bin/qidmap_cli.sh –i -f <filename>

   где <filename> — путь назначения файла sample_qid.txt, загруженного на шаге 2.
4. Для просмотра добавленных пользовательских QID, выполните следующую команду:

   /opt/qradar/bin/qidmap_cli.sh –e

В случае возникновения ошибки см. варианты решения проблемы в Руководстве администратора IBM QRadar.

Добавление Kaspersky CyberTrace Service в качестве источника журналов

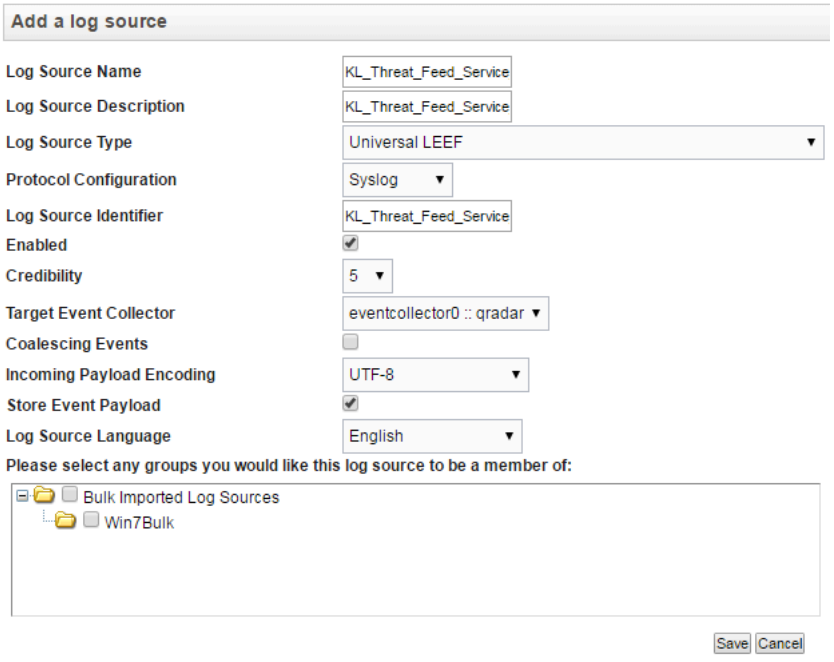
Чтобы события, отправляемые Kaspersky CyberTrace Service, поступали в QRadar, QRadar должен рассматривать Kaspersky CyberTrace Service как источник журналов. Kaspersky CyberTrace Service отправляет события в формате QRadar Log Event Extended Format (LEEF), а в качестве нового источника журналов в QRadar будет использоваться источник журналов Universal LEEF.

Чтобы добавить Kaspersky CyberTrace Service в QRadar в качестве источника журналов:

1. Выберите пункт меню **Admin** → **Log Sources** → **Add**.
2. В окне **Add a log source** введите уникальное имя для источника журналов.

   Это имя будет отображаться в графическом интерфейсе для всех событий из этого источника.
3. Введите описание источника журналов.
4. Выберите `Universal LEEF` в раскрывающемся списке **Log Source Type**.
5. Выберите **Syslog** в раскрывающемся списке **Protocol Configuration**.
6. В поле ввода **Log Source Identifier** введите идентификатор, заданный в конфигурационном файле Kaspersky CyberTrace Service; в данном случае это `KL_Threat_Feed_Service_v2`. Этот идентификатор используется в параметрах EventFormat и AlertFormat.

   Не устанавливайте флажок **Coalescing Events**. Если установить этот флажок, все события из Kaspersky CyberTrace Service будут объединяться в одно событие, не содержащее полезной информации.



Добавление источника журналов в QRadar

7. Нажмите на кнопку **Save**.

Выполните действия в том же порядке, чтобы добавить еще один источник журналов с идентификатором `KL_Verification_Tool`. Он будет использоваться для тестирования взаимодействия между Kaspersky CyberTrace Service и QRadar.

После добавления двух источников журналов выберите пункт меню **Admin** → **Deploy Changes**.

Если события не поступают на порт 514 сервера QRadar, выполните следующие команды с хоста, на котором установлен QRadar.

Выполните команду для консоли QRadar и подождите пять минут:

```
/opt/qradar/support/all_servers.sh -Ck 'if [ -f /opt/qradar/ecs/license.txt ] ; then echo
-n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" >
/opt/qradar/ecs/license.txt ; fi ; if [ -f /opt/ibm/si/services/ecs-ec-
ingress/current/eventgnosis/license.txt ] ; then echo -n "QRadar:Q1 Labs
Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/ibm/si/services/ecs-ec-
ingress/current/eventgnosis/license.txt ; fi ; if [ -f /opt/ibm/si/services/ecs-
ep/current/eventgnosis/license.txt ] ; then echo -n "QRadar:Q1 Labs
Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/ibm/si/services/ecs-
ep/current/eventgnosis/license.txt ; fi ; if [ -f /opt/ibm/si/services/ecs-
ec/current/eventgnosis/license.txt ] ; then echo -n "QRadar:Q1 Labs
Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/ibm/si/services/ecs-
ec/current/eventgnosis/license.txt ; fi ; if [ -f /usr/eventgnosis/ecs/license.txt ] ;
then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" >
/usr/eventgnosis/ecs/license.txt ; fi ; if [ -f
/opt/qradar/conf/templates/ecs_license.txt ] ; then echo -n "QRadar:Q1 Labs
Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" >
/opt/qradar/conf/templates/ecs_license.txt ; fi'
```

Выполните команду для QRadar Community Edition и подождите пять минут:

```
if [ -f /opt/qradar/ecs/license.txt ] ; then echo -n "QRadar:Q1 Labs
Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/qradar/ecs/license.txt ; fi ;
if [ -f /opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/license.txt ] ; then echo
-n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" >
/opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/license.txt ; fi ; if [ -f
/opt/ibm/si/services/ecs-ep/current/eventgnosis/license.txt ] ; then echo -n "QRadar:Q1
Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/ibm/si/services/ecs-
ep/current/eventgnosis/license.txt ; fi ; if [ -f /opt/ibm/si/services/ecs-
ec/current/eventgnosis/license.txt ] ; then echo -n "QRadar:Q1 Labs
Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/ibm/si/services/ecs-
ec/current/eventgnosis/license.txt ; fi ; if [ -f /usr/eventgnosis/ecs/license.txt ] ;
then echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" >
/usr/eventgnosis/ecs/license.txt ; fi ; if [ -f
/opt/qradar/conf/templates/ecs_license.txt ] ; then echo -n "QRadar:Q1 Labs
Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" >
/opt/qradar/conf/templates/ecs_license.txt ; fi
```

Сопоставление событий с QID

Когда события из файла sample_initiallog.txt поступают в QRadar, на странице **Log Activity** они могут отображаться с именем «unknown», «Unknown Kaspersky Threat Feed Service Event» или иным описательным именем вместо стандартного значения (например, «KL_Threat_Feed_Service» или «CyberCrime_Tracker_Block_Url»). Это может привести к дублированию несвязанных между собой событий.

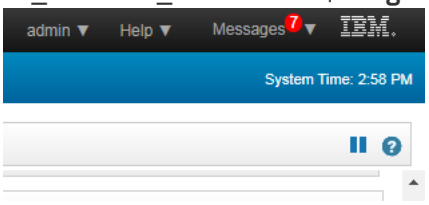
unknown	KL_Threat_Feed_Service_
unknown	KL_Threat_Feed_Service_
unknown	KL_Threat_Feed_Service_
unknown	KL_Threat_Feed_Service_
unknown	KL_Threat_Feed_Service_
unknown	KL_Threat_Feed_Service_
unknown	KL_Threat_Feed_Service_
unknown	KL_Threat_Feed_Service_
unknown	KL_Threat_Feed_Service_
unknown	KL_Threat_Feed_Service_
unknown	KL_Threat_Feed_Service_
unknown	KL_Threat_Feed_Service_
unknown	KL_Threat_Feed_Service_
unknown	KL_Threat_Feed_Service_
unknown	KL_Threat_Feed_Service_
unknown	KL_Threat_Feed_Service_
unknown	KL_Threat_Feed_Service_

Журнал с событиями «unknown»

Если на странице **Log Activity** отображается слишком много событий, поступающих с разных устройств, можно добавить фильтр событий. В этом фильтре событий установите `KL_Threat_Feed_Service_v2` и `KL_Verification_Tool` в качестве источников журналов (в фильтре должен использоваться оператор `Equals any of`).

Чтобы правильно идентифицировать события, настройте сопоставление QID с событиями:

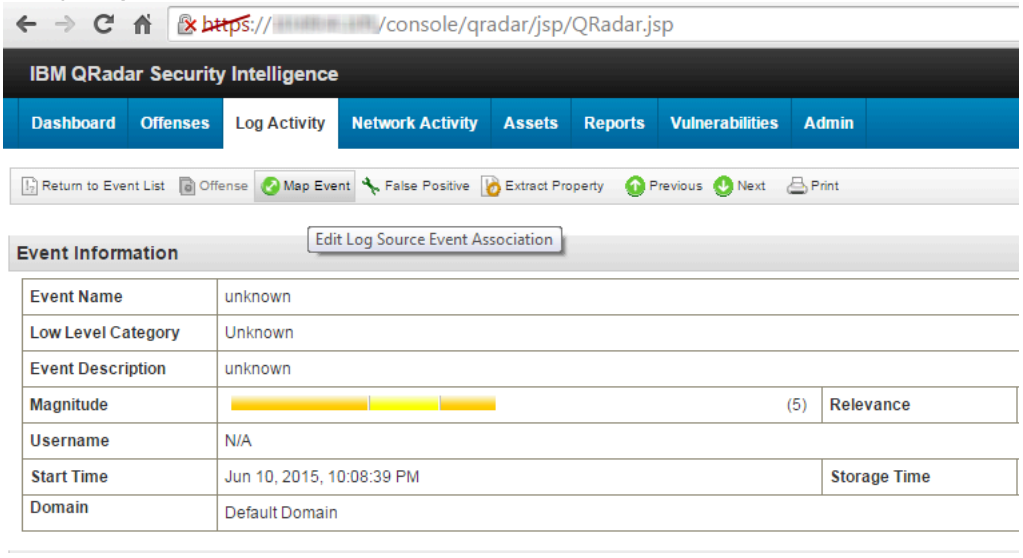
1. В QRadar Console выберите вкладку **Log Activity**, нажмите на кнопку **Pause** (⏸) в правом верхнем углу окна, чтобы остановить поток событий, затем дважды щелкните любое из событий с неправильным именем и значением "`KL_Threat_Feed_Service_v2`" в столбце **Log Source**.



Остановка потока событий

Отобразится информация о событии. Имя события содержится в поле **Payload information**.

2. Нажмите на кнопку **Map Event**.

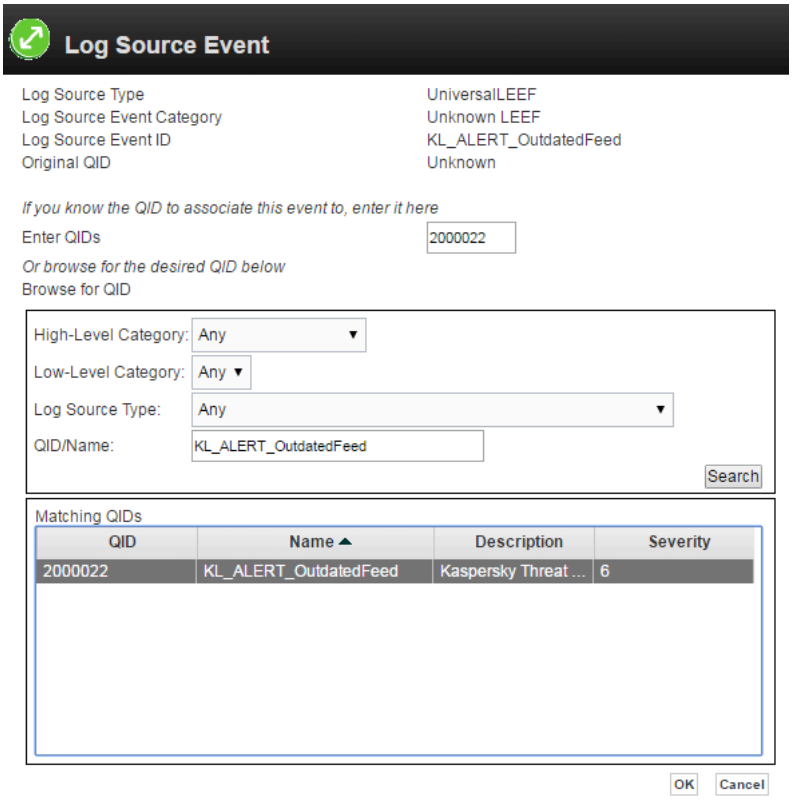


Просмотр информации о событии

3. В окне **Log Source Event** в поле ввода **QID/Name** введите имя события. Это должен быть один из QID, импортированных в QRadar.

4. Нажмите на кнопку **Search**.

   В таблице **Matching QIDs** будет отображаться один результат.



Добавление соответствия между QID и именем события

5. Выберите строку таблицы и нажмите кнопку **OK**.

6. Выполните шаги 3, 4 и 5 для всех типов событий (импортированных QID).

7. Чтобы убедиться, что сопоставление событий с QID выполняется правильно, повторите процедуру отправки набора событий в QRadar. На странице **Log Activity** не должно остаться событий с неправильным названием.

Current Filters:
Log Source is KL_Threat_Feed_Service_v2 (Clear Filter)

	Event Name	Log Source	Event Count	Time	Low Level Category
	KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address
	KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address
	KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address
	KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address
	KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address
	KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address
	KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address
	KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address
	KL_Malicious_Hash_MD5	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address
	KL_Malicious_Hash_SHA1	KL_Threat_Feed_Service_v2	1	Mar 23, 2016, 9:23:31 PM	Blacklist Address

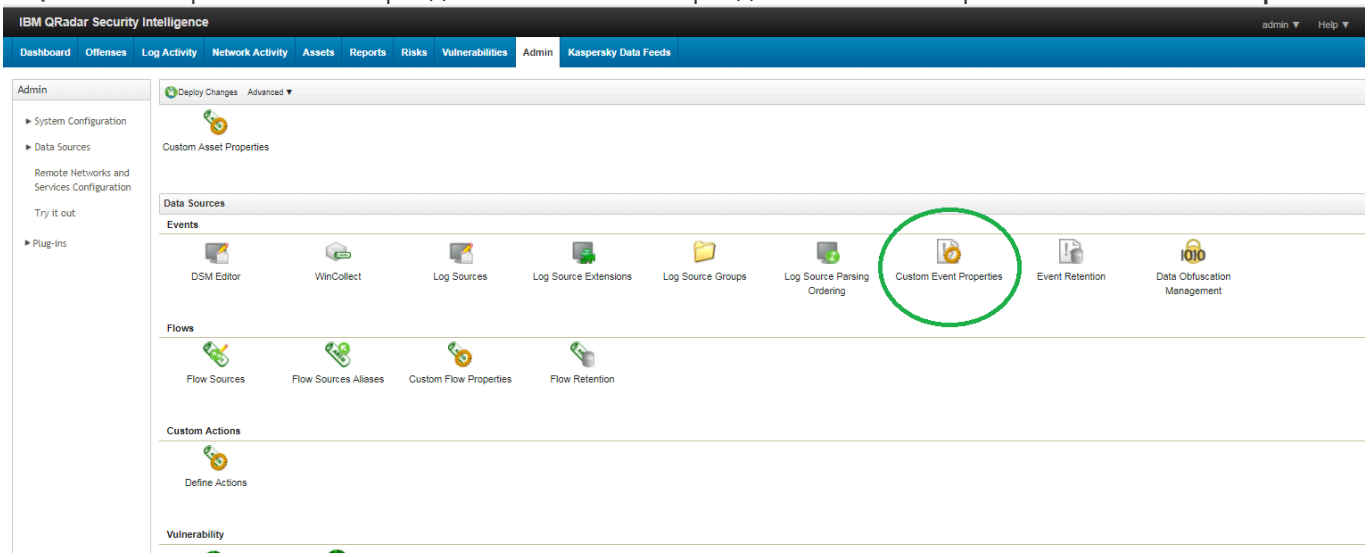
Журнал без событий «unknown»

Указание типа источника журналов

Следующая процедура требуется только в том случае, если пришлось вручную добавить Kaspersky CyberTrace Service в QRadar в качестве источника журналов из-за отсутствия последних обновлений QRadar. С помощью этой процедуры задается свойство `Log Source Type` добавленных пользовательских свойств события.

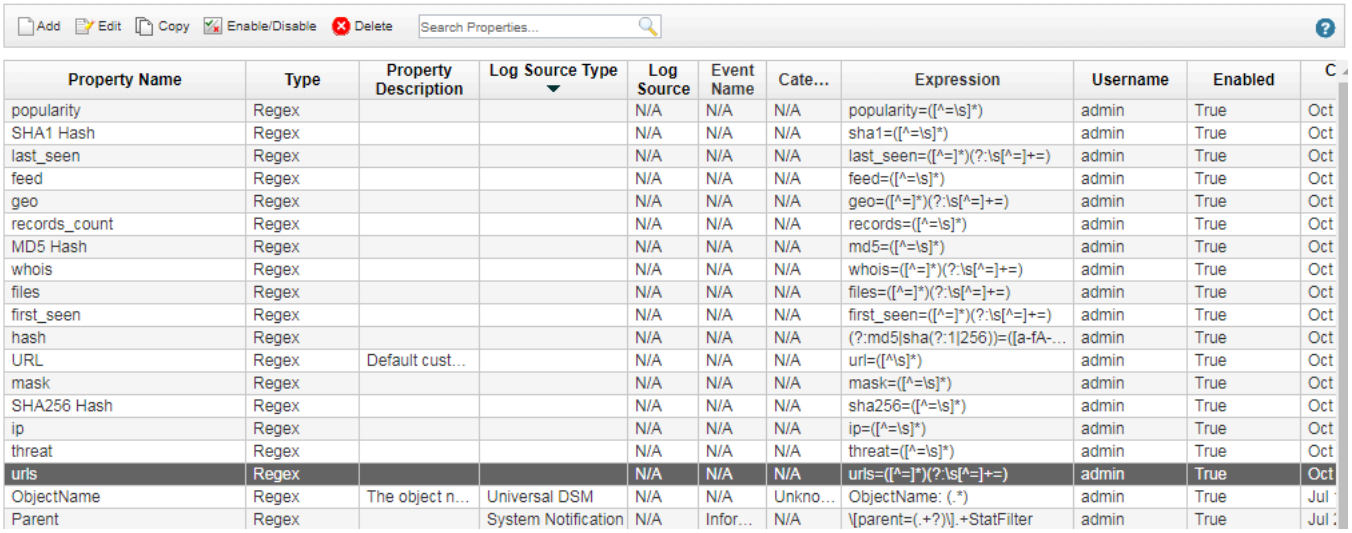
Чтобы указать тип источника журналов для добавленных пользовательских свойств события, выполните следующие действия:

1. В QRadar выберите **Admin** и в разделе **Data sources** в разделе **Events** выберите **Custom Event Properties**.



Вкладка **Admin** в QRadar Console

Откроется окно **Custom Event Properties**.



Property Name	Type	Property Description	Log Source Type	Log Source	Event Name	Cate...	Expression	Username	Enabled	C
popularity	Regex			N/A	N/A	N/A	popularity=([^=\s]*)	admin	True	Oct
SHA1 Hash	Regex			N/A	N/A	N/A	sha1=([^=\s]*)	admin	True	Oct
last_seen	Regex			N/A	N/A	N/A	last_seen=([^=]*)(?:\s[^=]+=)	admin	True	Oct
feed	Regex			N/A	N/A	N/A	feed=([^=\s]*)	admin	True	Oct
geo	Regex			N/A	N/A	N/A	geo=([^=]*)(?:\s[^=]+=)	admin	True	Oct
records_count	Regex			N/A	N/A	N/A	records=([^=\s]*)	admin	True	Oct
MD5 Hash	Regex			N/A	N/A	N/A	md5=([^=\s]*)	admin	True	Oct
whois	Regex			N/A	N/A	N/A	whois=([^=]*)(?:\s[^=]+=)	admin	True	Oct
files	Regex			N/A	N/A	N/A	files=([^=]*)(?:\s[^=]+=)	admin	True	Oct
first_seen	Regex			N/A	N/A	N/A	first_seen=([^=]*)(?:\s[^=]+=)	admin	True	Oct
hash	Regex			N/A	N/A	N/A	(?:md5|sha(?:1|256))=([a-fA-...	admin	True	Oct
URL	Regex	Default cust...		N/A	N/A	N/A	url=([^\s]*)	admin	True	Oct
mask	Regex			N/A	N/A	N/A	mask=([^=\s]*)	admin	True	Oct
SHA256 Hash	Regex			N/A	N/A	N/A	sha256=([^=\s]*)	admin	True	Oct
ip	Regex			N/A	N/A	N/A	ip=([^=\s]*)	admin	True	Oct
threat	Regex			N/A	N/A	N/A	threat=([^=\s]*)	admin	True	Oct
urls	Regex			N/A	N/A	N/A	urls=([^=]*)(?:\s[^=]+=)	admin	True	Oct
ObjectName	Regex	The object n...	Universal DSM	N/A	N/A	Unkno...	ObjectName: (.*)	admin	True	Jul
Parent	Regex		System Notification	N/A	Infor...	N/A	\[parent=(.+?)\].+StatFilter	admin	True	Jul

Пользовательские свойства события

2. Для каждого пользовательского свойства события выполните следующие действия:

   a. Выберите свойство.

   b. Нажмите на кнопку **Изменить**.

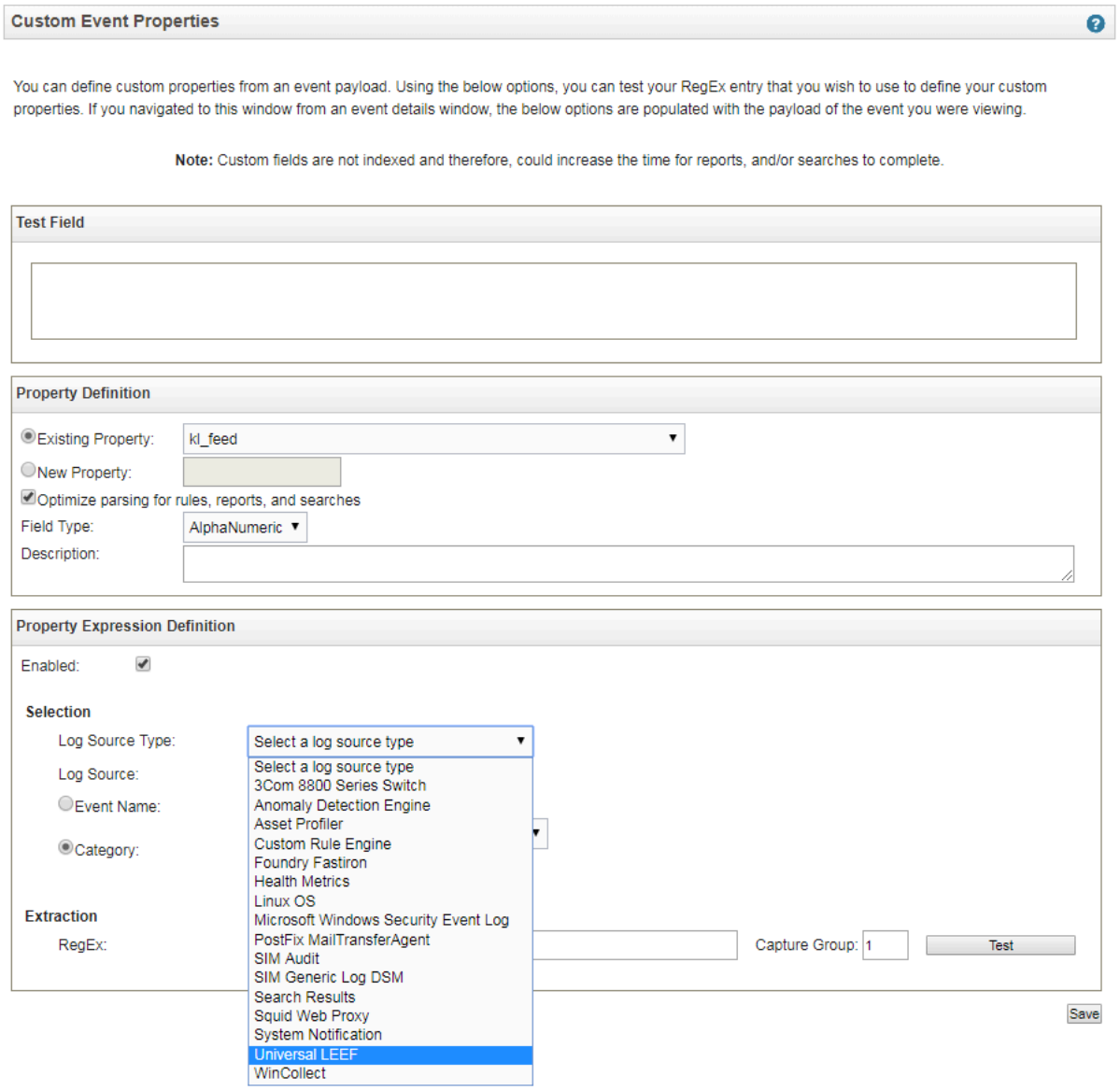
      Откроется окно **Custom Event Property Definition**.

   c. В раскрывающемся списке **Log Source Type** выберите **Universal LEEF**.

d. Выберите вариант **Existing Property**.

Вариант **Existing Property** был выбран до изменения значения в раскрывающемся списке **Log Source Type**. Однако после изменения типа источника журналов был выбран вариант **New Property**. Следовательно, необходимо снова выбрать вариант **Existing Property**.

e. Нажмите на кнопку **Save**.



Определение пользовательского свойства события

Теперь для всех пользовательских свойств события задан тип источника журналов «Universal LEEF».

Интеграция с RSA NetWitness

В этой главе описывается порядок интеграции Kaspersky CyberTrace с RSA NetWitness.

RSA NetWitness

В этой главе описывается порядок интеграции Kaspersky CyberTrace с RSA NetWitness.

О схемах интеграции

Для интеграции Kaspersky CyberTrace с RSA NetWitness рекомендуется стандартная схема интеграции.

Порядок интеграции с RSA NetWitness

Перед началом интеграции Kaspersky CyberTrace с RSA NetWitness необходимо выполнить следующие действия:

- Перед установкой Kaspersky CyberTrace убедитесь, что службы RSA NetWitness соответствуют программным требованиям.
- Убедитесь, что выполнена установка Kaspersky CyberTrace.

Чтобы интегрировать Kaspersky CyberTrace с RSA NetWitness, выполните следующие действия:

- Шаг 1. Настройка в RSA NetWitness пересылки получаемых событий в Kaspersky CyberTrace Service.
- Шаг 2. Настройка в RSA NetWitness получение событий от Kaspersky CyberTrace Service.
- Шаг 3 (необязательный). Импорт метагруппы для просмотра всех полей в RSA NetWitness, которые заполняет Kaspersky CyberTrace Service.
- Шаг 4 (необязательный). Импорт правил Kaspersky CyberTrace Service в RSA NetWitness.
- Шаг 5 (необязательный). Импорт предварительно настроенного отчета в RSA NetWitness.

  Для выполнения этого шага необходимо импортировать правила Kaspersky CyberTrace Service (шаг 4).
- Шаг 6 (необязательный). Импорт предварительно настроенных диаграмм и информационной панели в RSA NetWitness.

  Для выполнения этого шага необходимо импортировать правила Kaspersky CyberTrace Service (шаг 4).
- Шаг 7. Выполните проверку работоспособности.

  Перед изменением каких-либо настроек процесса сопоставления необходимо выполнить проверку работоспособности.

Предварительные условия (RSA NetWitness)

В этом разделе описываются дополнительные требования, которые необходимо удовлетворить перед интеграцией Kaspersky CyberTrace с RSA NetWitness.

Проверка настройки программного обеспечения (RSA NetWitness)

В этом разделе описываются требования к службам RSA NetWitness.

Убедитесь, что выполняются следующие условия:

- Файл индекса (index-concentrator-custom.xml) Concentrator, получающий события Kaspersky CyberTrace Service, должен содержать следующие метаполя:

  - `virusname`

    Это и другие метаполя (за исключением `msg`) должны иметь уровень `IndexValues`. Кроме того, для параметра `defaultAction` этих метаполей установите значение `Open`.

  - `user.src`
  - `ip.src`
  - `action`
  - `msg`

    Это метаполе должно иметь уровень `IndexKeys` (наличие метаполя в событии индексируется) или `IndexNone` (метаполе не индексируется) в файле index-concentrator-custom.xml. Если для метаполя задан уровень `IndexValues`, пространство на жестком диске будет расходоваться быстрее.

  - `event.source`
  - `device.ip`
  - `ip.dst`
  - `url`
  - `checksum`

  Если какие-либо из этих полей отсутствуют в индексном файле, добавьте их в файл и перезагрузите Concentrator, как описано в разделе об устранении неполадок RSA NetWitness.

  Если Concentrator отсутствует, но для хранения данных из Kaspersky CyberTrace Service используется Log Decoder, измените файл index-logdecoder-custom.xml и перезапустите Log Decoder, как описано выше.

  > Если Concentrator получает данные от Log Decoder, обновлять следует только индексный файл Concentrator (index-concentrator-custom.xml). Дополнительные сведения см. на странице https://community.rsa.com/docs/DOC-41760. Кроме того, обновить файл индекса Log Decoder (index-logdecoder-custom.xml) следует, если Log Decoder используется в качестве источника данных, в котором выполняется поиск событий, или если Log Decoder используется для создания отчетов или информационных панелей.

- Конфигурационный файл table-map-custom.xml (конфигурационный файл Log Decoder) должен содержать следующие метаполя:

  - `virusname`
  - `c_username`
  - `saddr`
  - `daddr`

- `url`
- `checksum`
- `msg`
- `event_source`
- `hostip`
- `action`

Для каждого из этих метаполей атрибут `flags` должен иметь значение `None`.

Если в индексных файлах отсутствует какое-либо из этих полей, см. раздел об устранении неполадок RSA NetWitness.

События обнаруженных киберугроз, отправляемые Kaspersky CyberTrace Service, содержат контекст из потоков данных об угрозах в отдельных полях. Эти поля могут отображаться и использоваться в RSA NetWitness. (В RSA NetWitness имена этих полей получают префикс `kl`).

Чтобы отобразить поля контекста, выполните следующие действия:

1. Добавьте содержимое файла `%service_dir%/integration/rsa/additional_elements/table-map-custom.xml` в файл `table-map-custom.xml` Log Decoder, в который Kaspersky CyberTrace Service будет отправлять события обнаруженных киберугроз.
2. Добавьте содержимое файла `%service_dir%/integration/rsa/additional_elements/index-concentrator-custom.xml` в файл `index-concentrator-custom.xml` Concentrator, в котором будут храниться события из Kaspersky CyberTrace Service.

Все настройки, описанные выше, можно задать в веб-интерфейсе RSA NetWitness на экране **Services** (Log Decoder and Concentrator) → **Config**.

После внесения изменений в файлы table-map-custom.xml и index-concentrator-custom.xml перезагрузите Log Decoder и Concentrator.

Стандартная интеграция (RSA NetWitness)

В этом разделе описывается порядок интеграции Kaspersky CyberTrace и RSA NetWitness по стандартной схеме интеграции.

О стандартной схеме интеграции (RSA NetWitness)

В этом разделе описывается стандартная схема интеграции RSA NetWitness и Kaspersky CyberTrace.

О компонентах стандартной схемы интеграции

В стандартной схеме интеграции RSA NetWitness используются следующие компоненты:

- Kaspersky CyberTrace Service

  Эта служба сопоставляет события RSA NetWitness с потоками данных об угрозах Kaspersky Threat Data Feeds.

- RSA NetWitness

  SIEM-система, используемая в этой интеграции.

- Средства контроля безопасности

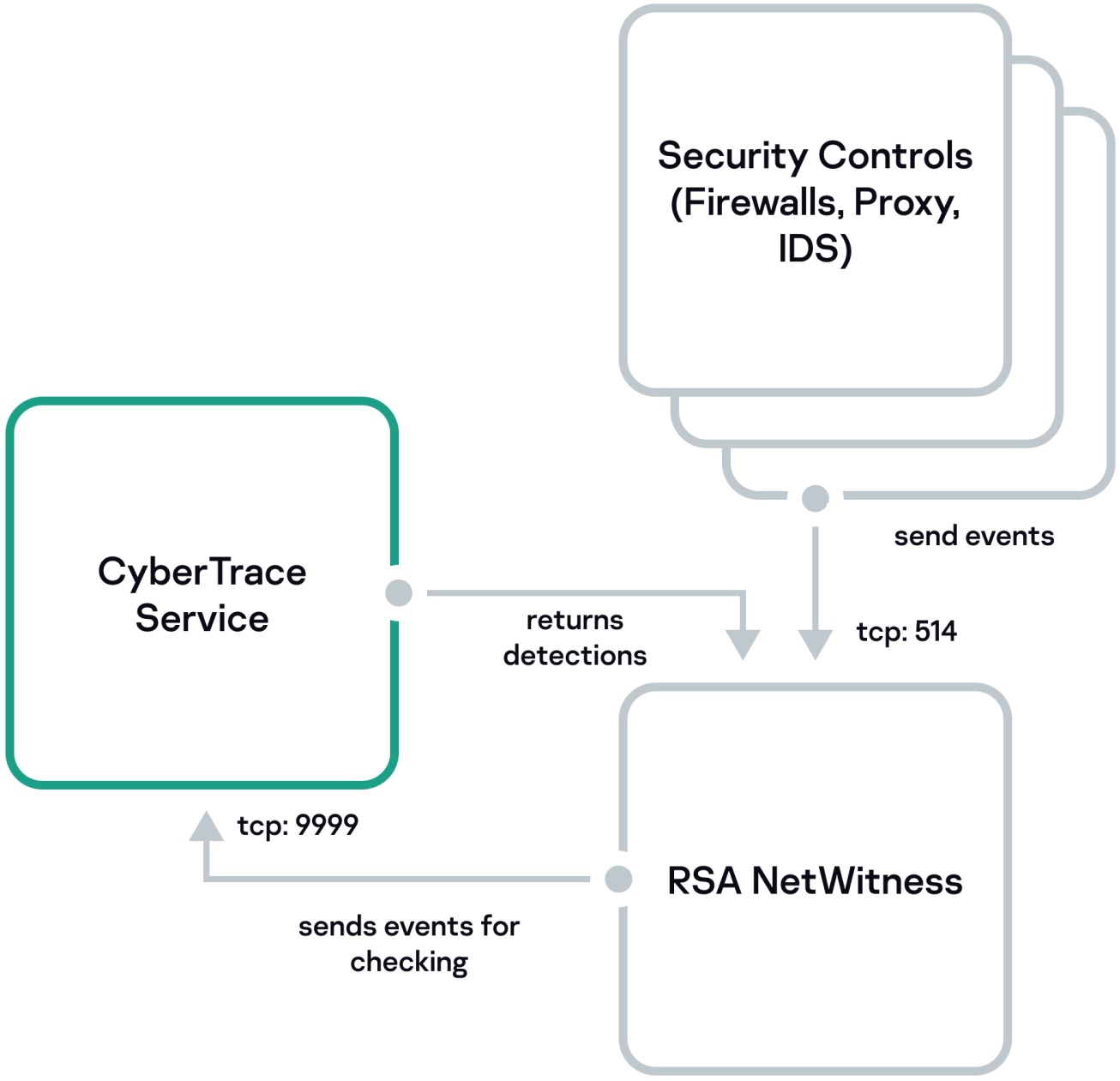
  Это источники событий для RSA NetWitness, такие как межсетевые экраны, прокси-серверы, системы обнаружения вторжений и другие сетевые устройства.

  Средства контроля безопасности могут отправлять события в RSA NetWitness любым способом, поддерживаемым RSA NetWitness.

Стандартная схема интеграции

В стандартной схеме интеграции Kaspersky CyberTrace Service по умолчанию настраивается на прослушивание адреса `127.0.0.1:9999` для получения входящих событий от RSA NetWitness.

Kaspersky CyberTrace Service отправляет события обнаруженных киберугроз на IP-адрес `127.0.0.1` и порт `514` интерфейса, определенного в конфигурации RSA NetWitness. Адрес этого интерфейса указывается при установке Kaspersky CyberTrace. Средства контроля безопасности также отправляют события на порт 514 интерфейса, определенного в конфигурации RSA NetWitness.



Стандартная схема интеграции для RSA NetWitness

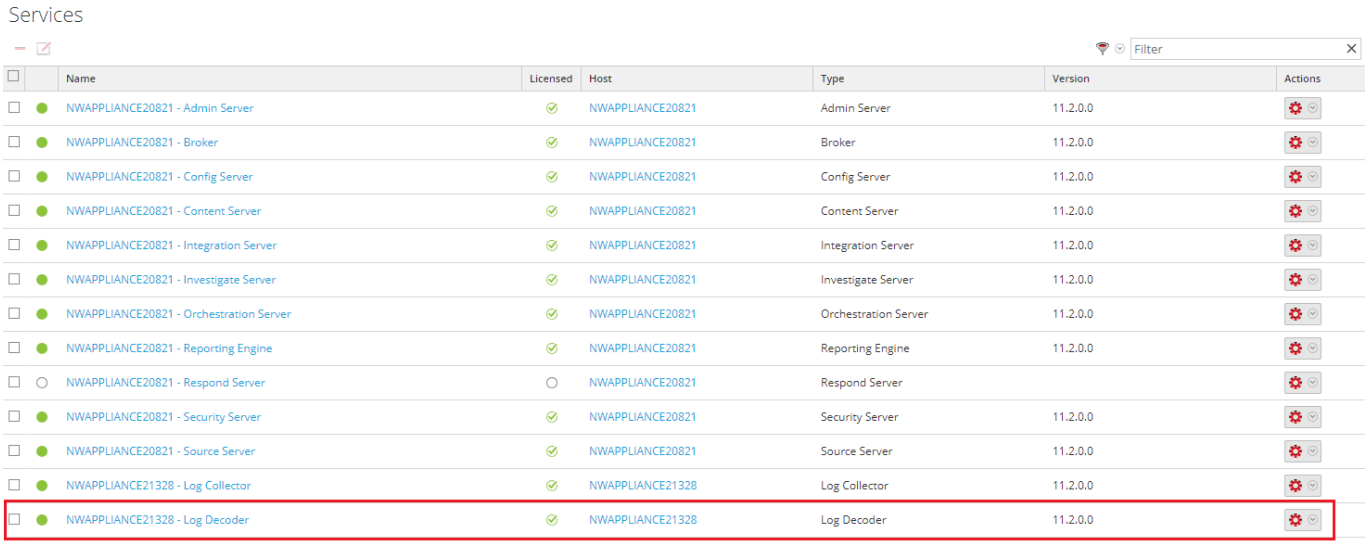
Шаг 1. Пересылка событий из RSA NetWitness

В этом разделе описывается порядок настройки в RSA NetWitness пересылки получаемых событий в Kaspersky CyberTrace Service.

Чтобы пересылать события из RSA NetWitness в Kaspersky CyberTrace Service, выполните следующие действия:

1. В главном окне RSA NetWitness выберите **(Admin)** → **System**.

2. В таблице **Services** ниже выберите соответствующий Log Decoder (Log Decoder, который получает события, содержащие URL, хеш или IP-адрес).



Выбор Log Decoder

Если для приема событий используется более одного Log Decoder, повторите следующие шаги для каждого Log Decoder.

3. Для выбранного Log Decoder в столбце **Actions** нажмите кнопку **Settings** (), затем в раскрывающемся списке выберите **View** → **Config**.

4. Перейдите на вкладку **App Rules** и нажмите кнопку **Add** (**+**).

   Откроется окно **Rule Editor**.

5. Укажите следующие данные:

   - **Rule Name**: `cybertrace`

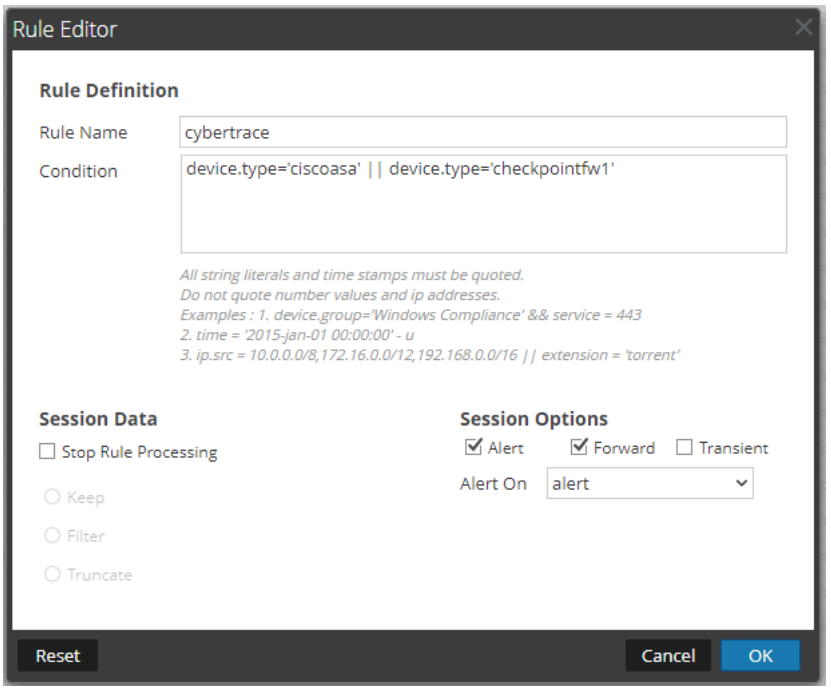
   - **Condition**: `device.type='%DEVICE_NAME_1%'`

     Это пример условия, в котором строка `%DEVICE_NAME_1%` представляет собой имя устройства, события которого должны отправляться в Kaspersky CyberTrace Service. Ниже приведен еще один пример условия, в соответствии с которым события из Cisco™ ASA и Check Point Firewall должны отправляться в Kaspersky CyberTrace Service:

     ```
     device.type='ciscoasa' || device.type='checkpointfw1'
     ```

     Если событие соответствует указанному здесь условию, оно отправляется в Kaspersky CyberTrace Service.

- **Alert**: флажок установлен
- **Forward**: флажок установлен



Окно Rule Editor

Дополнительные сведения о порядке создания правил см. на странице https://community.rsa.com/t5/rsa-netwitness-platform-online/configure-application-rules/ta-p/592148.

6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **Apply**.
8. Рядом с именем Log Decoder выберите **Config** → **Explore**.
9. Укажите назначение.

   - Для RSA NetWitness версии 11.2 и более поздних:

     В параметре **/decoder/config/logs.forwarding.destination** укажите следующее назначение:

     `cybertrace=tcp:[IP]:[port]:rfc3164`

     Здесь `[IP]` — это IP-адрес сервера, на котором установлен Kaspersky CyberTrace Service, а `[port]` — это порт, который Kaspersky CyberTrace Service прослушивает для получения событий (по умолчанию используется порт `9999`). IP-адрес и порт совпадают с указанными на странице **Параметры → Общие** веб-интерфейса Kaspersky CyberTrace.

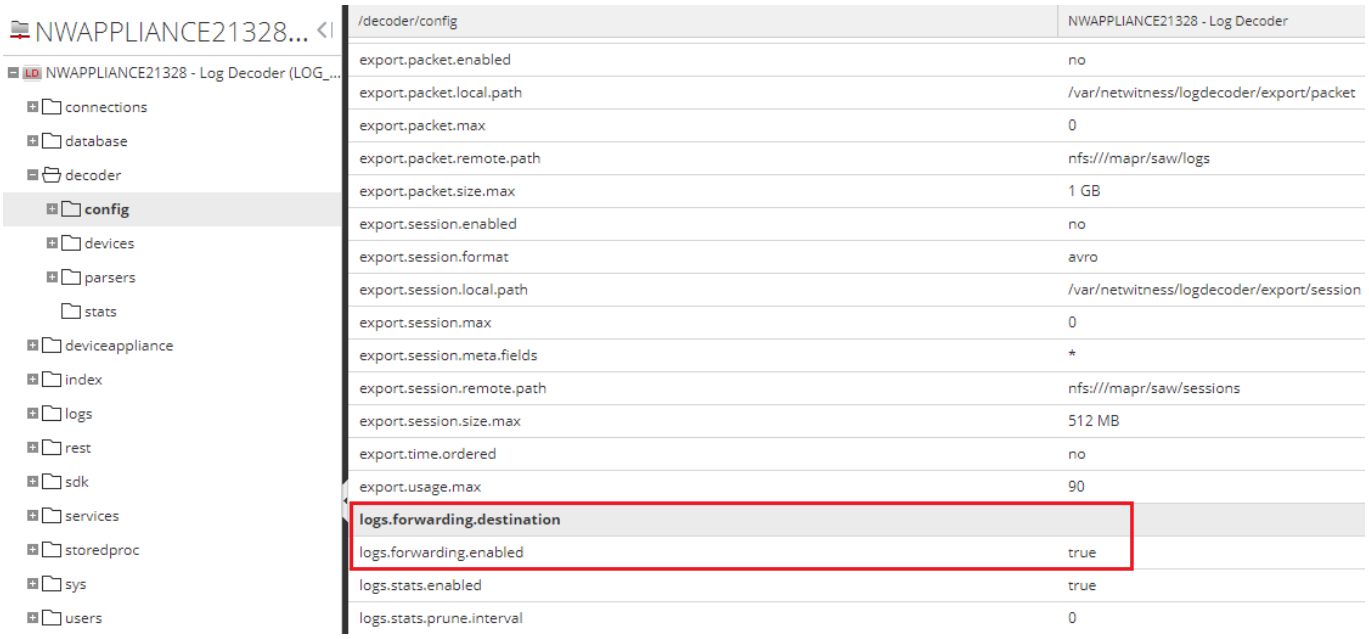
   - Для более ранних версий RSA NetWitness, чем 11.2:

     a. В параметре **/decoder/config/logs.forwarding.destination** укажите следующее назначение:

     `cybertrace=tcp:[IP]:[port]`

Здесь `[IP]` — это IP-адрес сервера, на котором установлен Kaspersky CyberTrace Service, а `[port]` — это порт, который Kaspersky CyberTrace Service прослушивает для получения событий (по умолчанию используется порт `9999`). IP-адрес и порт совпадают с указанными на странице **Параметры → Общие** веб-интерфейса Kaspersky CyberTrace.

b. Для параметра EventDelimeter в конфигурационном файле Kaspersky CyberTrace Service задайте значение `<![CDATA[(\<\d+\>)]]>`.



Параметры пересылки событий журнала

10. Для параметра **/decoder/config/logs.forwarding.enabled** задайте значение `true`.

После выполнения этих действий RSA NetWitness будет перенаправлять события, удовлетворяющие правилу `cybertrace`, на адрес, указанный в параметре `logs.forwarding.destination`.

Дополнительные сведения о пересылке событий см. на странице https://community.rsa.com/t5/rsa-netwitness-platform-online/decoder-configure-syslog-forwarding-to-destination/ta-p/572084.

Шаг 2. Отправка событий из Kaspersky CyberTrace Service в RSA NetWitness

В этом разделе описываются действия, которые необходимо совершить для настройки пересылки событий из Kaspersky CyberTrace Service в RSA NetWitness.

Обратите внимание, что Kaspersky CyberTrace Service отправляет события в службу Log Decoder.

Чтобы события из Kaspersky CyberTrace Service отправлялись в RSA NetWitness, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace на странице **Параметры → Служба** укажите следующее значение в поле ввода **Служебные оповещения**:

   `[IP]:514`

   Здесь `[IP]` — это IP-адрес службы Log Decoder, в который Kaspersky CyberTrace Service будет отправлять события.

   Если имеется несколько служб Log Decoder, интеграцию следует выполнять только с одной из служб Log Decoder.

2. В каталоге `/etc/netwitness/ng/envision/etc/devices` сервера, на котором работает Log Decoder, создайте подкаталог `cybertrace` и скопируйте в этот подкаталог следующие файлы из каталога `%service_dir%/integration/rsa/cybertrace`:

   - cybertrace.ini

     Этот конфигурационный файл содержит декларацию Kaspersky CyberTrace Service для RSA NetWitness.

   - v20_cybertracemsg.xml

     Этот конфигурационный файл содержит правила парсинга событий, отправляемых из Kaspersky CyberTrace Service в RSA NetWitness. Описание содержимого приведено далее в этом разделе.

   Эти файлы расположены в каталоге `integration/rsa/cybertrace` в комплекте поставки.

3. Перезапустите Log Decoder.

   Для этого на экране **Services** для выбранного Log Decoder нажмите на кнопку **Settings** (⚙) и в раскрывающемся списке выберите **Restart**.

4. Убедитесь, что в RSA NetWitness включен парсер службы `cybertrace`.

   Это можно сделать следующим образом:

   a. В меню RSA NetWitness выберите **(Admin)** → **System**.

   b. В таблице **Services** выберите Log Decoder и в меню **Actions** выберите **View** → **Config**.

   c. На панели **Service Parsers Configuration** найдите **cybertrace** и убедитесь, что в этой строке выбрано поле **Config Value**.

Service Parsers Configuration

Name	Config Value
crossbeamc	☑
cyberark	☑
cyberguardclassic	☑
cyberoamutm	☑
cybertrace	☑

Таблица «Service Parsers Configuration»

5. Перезапустите Kaspersky CyberTrace Service.

   Для перезапуска Kaspersky CyberTrace Service можно выполнить скрипт kl_feed_service:

   ```
   systemctl restart cybertrace.service
   ```

   Это также можно сделать и в веб-интерфейсе Kaspersky CyberTrace.

Содержимое файлов интеграции

Файл v20_cybertracemsg.xml содержит следующее правило для парсинга служебных событий из Kaspersky CyberTrace Service:

```
alert=&lt;action&gt;,context=&lt;msg&gt;
```

Файл v20_cybertracemsg.xml содержит несколько правил для парсинга событий обнаружения киберугроз, поступающих от Kaspersky CyberTrace Service:

- MATCH_EVENT:01 — для парсинга событий обнаруженных киберугроз при использовании Botnet C&C URL Data Feed в процессе обнаружения киберугроз.
- MATCH_EVENT:02 — для парсинга событий обнаруженных киберугроз при использовании Malicious URL Data Feed в процессе обнаружения киберугроз.
- MATCH_EVENT:03 — для парсинга событий обнаруженных киберугроз при использовании Mobile Botnet C&C URL Data Feed в процессе обнаружения киберугроз.
- MATCH_EVENT:04 — для парсинга событий обнаруженных киберугроз при использовании Malicious Hash Data Feed в процессе обнаружения киберугроз.
- MATCH_EVENT:05 — для парсинга событий обнаруженных киберугроз при использовании Phishing URL Data Feed в процессе обнаружения киберугроз.
- MATCH_EVENT:06 — для парсинга событий обнаруженных киберугроз при использовании Ransomware URL Data Feed или IoT URL Data Feed в процессе обнаружения киберугроз.
- MATCH_EVENT:07 — для парсинга событий обнаруженных киберугроз при использовании IP Reputation Data Feed в процессе обнаружения киберугроз.
- MATCH_EVENT:09 — для парсинга событий обнаруженных киберугроз при использовании Mobile Malicious Hash Data Feed в процессе обнаружения киберугроз.
- MATCH_EVENT:10 — для парсинга событий обнаруженных киберугроз при использовании APT IP Data Feed и URL Data Feed в процессе обнаружения киберугроз.
- MATCH_EVENT:11 — для парсинга событий обнаруженных киберугроз при использовании Industrial Control Systems Data Feed в процессе обнаружения киберугроз.
- MATCH_EVENT:12 — для парсинга событий обнаруженных киберугроз при использовании APT Hash Data Feed в процессе обнаружения киберугроз.
- MATCH_EVENT — для парсинга событий обнаруженных киберугроз при использовании прочих потоков данных об угрозах в процессе обнаружения киберугроз.

Поля файлов cybertrace.ini и v20_cybertracemsg.xml соответствуют следующему формату служебных событий и событий обнаружения киберугроз из Kaspersky CyberTrace Service:

```
<AlertFormat><![CDATA[<232>%CyberTrace:ALERT_EVENT alert=%Alert%,context=%RecordContext%]]></AlertFormat>
<EventFormat><![CDATA[<232>%CyberTrace:MATCH_EVENT
category=%Category%,detected=%MatchedIndicator%,url=%RE_URL%,hash=%RE_HASH%,dst=%DST_IP%,src=%SRC_IP%,dvc=%DeviceIp%,
</EventFormat>
```

В файле v20_cybertracemsg.xml формат событий из Kaspersky CyberTrace Service задается в элементе `HEADER/content` и в элементе `MESSAGE/content`. Убедитесь, что в файлах индекса Log Decoder и Concentrator присутствуют следующие поля: `virusname`, `url`, `checksum`, `ip.src`, `ip.dst`. Другие поля (кроме `virusname`, `url`, `checksum`, `ip.src`, `ip.dst` в элементе `MESSAGE/content`) можно как использовать, так и не использовать в файлах индекса Log Decoder и Concentrator. Также убедитесь, что в файле table-map-custom.xml для каждого из этих полей для атрибута `flags` задано значение `None`. Если какое-либо из этих условий не выполняется, см. раздел об устранении неполадок RSA NetWitness.

В следующих таблицах описаны поля, используемые в файлах v20_cybertracemsg.xml и kl_feed_service.conf, и соответствие между полями в этих двух файлах. Если какое-либо новое поле требуется постоянно использовать в событиях обнаружения киберугроз, обратитесь по адресу intelligence@kaspersky.com.

- Поля служебных событий

Поле в kl_feed_service.conf	Поле в v20_cybertracemsg.xml	Описание
<232>	-	Строка службы для RSA NetWitness.
%CyberTrace:	%CyberTrace:	Информирует RSA NetWitness о том, что из Kaspersky CyberTrace Service отправлено событие.
ALERT_EVENT	<messageid>	Тип события.
-	<!payload>	Уведомляет RSA NetWitness о том, что событие содержит дополнительные данные, формат которых указан в элементе `MESSAGE/content` element.
%Alert%	<action>	Служебное событие (например, KL_ALERT_ServiceStarted).
%RecordContext%	<msg>	Контекстные данные о служебном событии.

- Поля событий обнаруженных киберугроз

Поле в kl_feed_service.conf	Поле в v20_cybertracemsg.xml	Описание
<232>	-	Строка службы для RSA NetWitness.
%CyberTrace:	%CyberTrace:	Информирует RSA NetWitness о том, что из Kaspersky CyberTrace Service отправлено событие.
MATCH_EVENT	<messageid>	Тип события.
-	<!payload>	Уведомляет RSA NetWitness о том, что событие содержит дополнительные данные, формат которых указан в элементе `MESSAGE/content` element.
%Category%	<virusname>	Категория обнаруженного объекта.
%MatchedIndicator%	<kl_detected_indicator%gt;	Обнаруженный индикатор.
%RE_URL%	<url>	URL, указанный в событии от RSA NetWitness.
%RE_HASH%	<checksum>	Хеш, указанный в событии от RSA NetWitness.
%DST_IP%	<daddr>	IP-адрес, на который отправляется запрос.
%SRC_IP%	<saddr>	IP-адрес, с которого отправляется запрос.
%DeviceIp%	<hostip>	IP-адрес, с которого отправляется событие.
%Device%	<event_source>	Имя устройства, отправившего событие.
%DeviceAction%	<action>	Действие, которое выполнило устройство.
%UserName%	<c_username>	Имя пользователя, с учетной записью которого выполняется действие, описанное в событии.
%ActionableFields%	Имена полей объясняются ниже в этом разделе.	Поля записи потока данных об угрозах, используемые в процессе обнаружения киберугроз, отображаются отдельно от контекста.
%RecordContext%	<fld1>	Контекст записи потока данных об угрозах, которая использовалась в процессе обнаружения киберугроз. Чтобы просмотреть содержимое этого поля, откройте событие в RSA NetWitness и выберите вкладку **View Log**.
%Confidence%	<kl_confidence>	Уровень доверия (в процентах) к индикаторам потока данных об угрозах.

В следующих таблицах описаны поля контекста, используемые в потоках данных и в файле v20_cybertracemsg.xml, а также соответствие полей потоке данных полям в файле:

- Botnet C&C URL Data Feed и Demo Botnet C&C URL Data Feed

Поле в потоке данных об угрозах	Поле в v20_cybertracemsg.xml
mask	kl_mask
first_seen	kl_first_seen
last_seen	kl_last_seen
popularity	kl_popularity
threat	kl_threat

- Malicious Hash Data Feed и Demo Malicious Hash Data Feed

Поле в потоке данных об угрозах	Поле в v20_cybertracemsg.xml
MD5	kl_md5
SHA1	kl_sha1
SHA256	kl_sha256
first_seen	kl_first_seen
last_seen	kl_last_seen
popularity	kl_popularity
file_type	kl_file_type
file_size	kl_file_size
threat	kl_threat

- IP Reputation Data Feed и Demo IP Reputation Data Feed

Поле в потоке данных об угрозах	Поле в v20_cybertracemsg.xml
ip	kl_ip
first_seen	kl_first_seen
last_seen	kl_last_seen
popularity	kl_popularity
threat_score	kl_threat_score
category	kl_category
threat	kl_threat

- Malicious URL Data Feed

Поле в потоке данных об угрозах	Поле в v20_cybertracemsg.xml
mask	kl_mask
first_seen	kl_first_seen
last_seen	kl_last_seen
popularity	kl_popularity
files/threat	kl_threat
category	kl_category

- Mobile Malicious Hash Data Feed

Поле в потоке данных об угрозах	Поле в v20_cybertracemsg.xml
MD5	kl_md5
SHA1	kl_sha1
SHA256	kl_sha256
first_seen	kl_first_seen

last_seen	kl_last_seen
popularity	kl_popularity
threat	kl_threat
file_size	kl_file_size

- Phishing URL Data Feed

Поле в потоке данных об угрозах	Поле в v20_cybertracemsg.xml
mask	kl_mask
first_seen	kl_first_seen
last_seen	kl_last_seen
popularity	kl_popularity
industry	kl_industry

- Mobile Botnet C&C URL Data Feed

Поле в потоке данных об угрозах	Поле в v20_cybertracemsg.xml
threat	kl_threat

- Ransomware URL Data Feed или IoT URL Data Feed

Поле в потоке данных об угрозах	Поле в v20_cybertracemsg.xml
mask	kl_mask
first_seen	kl_first_seen
last_seen	kl_last_seen
popularity	kl_popularity

- APT IP Data Feed и APT URL Data Feed

Поле в потоке данных об угрозах	Поле в v20_cybertracemsg.xml
detection_date	kl_detect_date
publication_name	kl_pub_name

- APT Hash Data Feed

Поле в потоке данных об угрозах	Поле в v20_cybertracemsg.xml
detection_date	kl_detect_date
publication_name	kl_pub_name
SHA1	kl_sha1
SHA256	kl_sha256

- Industrial Control Systems Data Feed

Поле в потоке данных об угрозах	Поле в v20_cybertracemsg.xml
first_seen	kl_first_seen
popularity	kl_popularity

Шаг 3 (необязательный). Импорт метагруппы для просмотра полей, заполненных Kaspersky CyberTrace Service

В этом разделе описывается порядок импорта файла MetaGroups.jsn. Этот файл содержит метагруппу, которую можно использовать для просмотра только тех полей в RSA NetWitness, которые заполняет Kaspersky CyberTrace Service.

Дистрибутив Kaspersky CyberTrace содержит файл `integration/rsa/additional_elements/MetaGroups.jsn`. Этот файл содержит поля с именами вида `kl.%field_name%`. Если поля Kaspersky CyberTrace не были добавлены в RSA NetWitness (а именно в файлы table-map-custom.xml и index-concentrator-custom.xml), рекомендуется импортировать файл MetaGroups_without_kl_fields.jsn, а не файл MetaGroups.jsn.

Чтобы импортировать файл MetaGroups.jsn, выполните следующие действия:

1. Убедитесь, что в RSA NetWitness включен экран **Navigate**.

   По умолчанию в RSA NetWitness версии 11.6 и более поздних экран **Navigate** отключен. Чтобы включить экран **Navigate**, выполните следующие действия:

   a. Перейдите в раздел (**Admin**) → **System** → **Investigation** → **Navigate**.

   В версии 11.6.0 перейдите в раздел (**Admin**) → **System** → **Investigation** → **Investigate**.

   b. Установите флажок **Enable Navigate**.

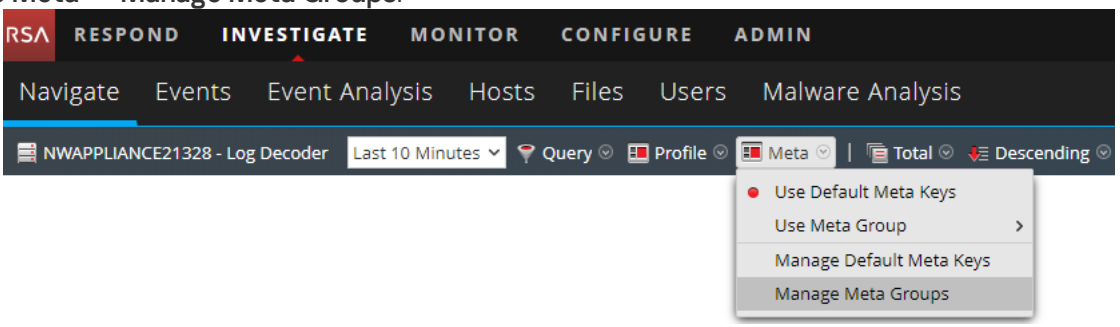
   c. Нажмите на кнопку **Apply**.

2. В меню RSA NetWitness выберите **Investigation** → **Navigate**.

   В версии 11.6.0 выберите **Investigate** → **Navigate**.

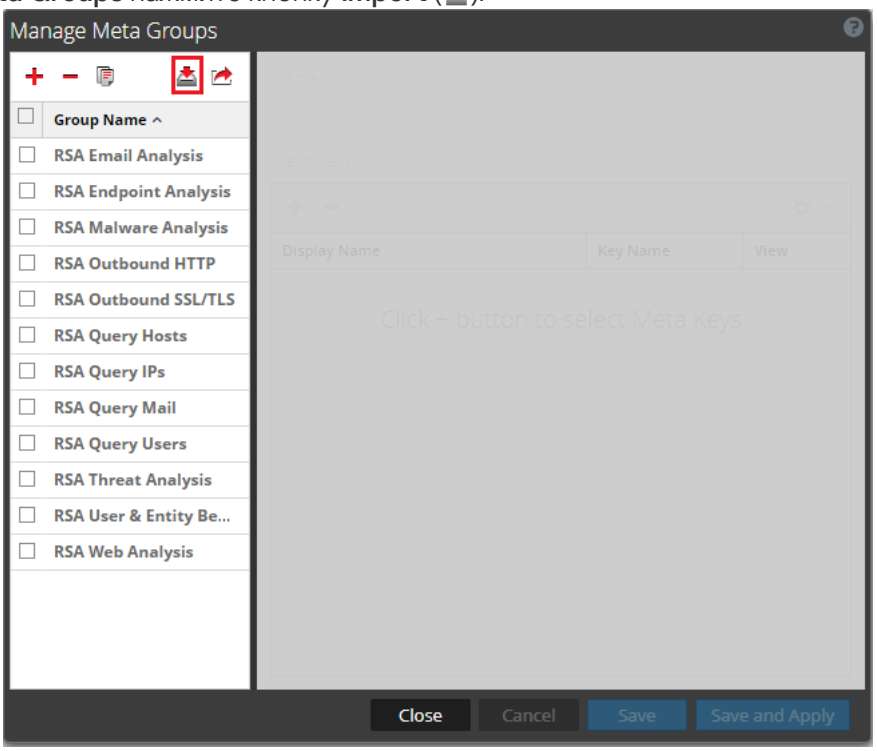
   Откроется окно **Investigate**.

3. Выберите **Meta** → **Manage Meta Groups**.



Команда **Manage Meta Groups**

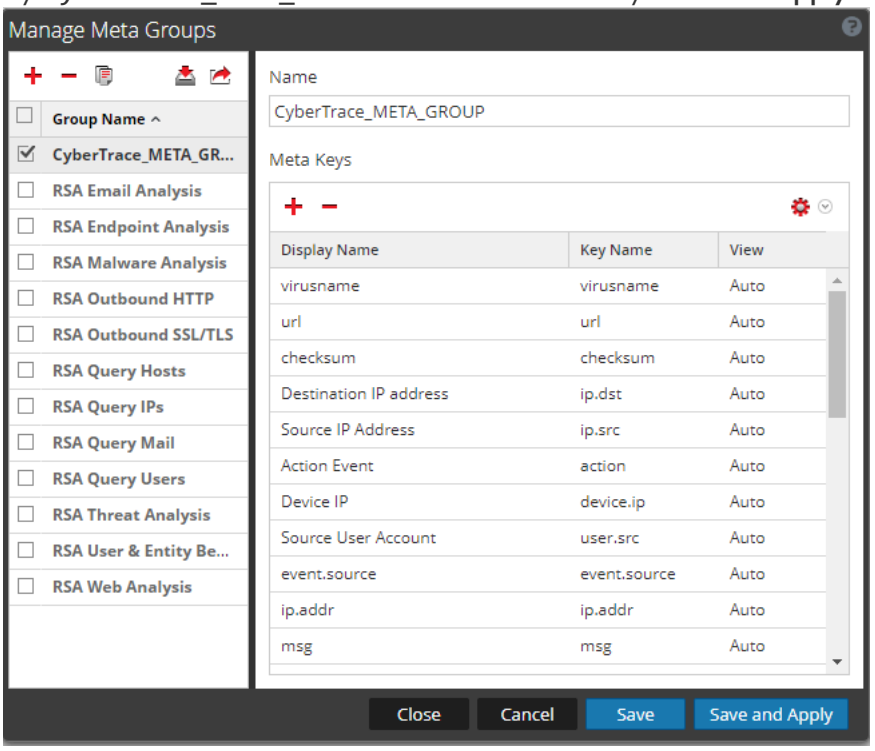
4. В окне **Manage Meta Groups** нажмите кнопку **Import** ( ).



Окно **Manage Meta Groups**

5. Выберите файл MetaGroups.jsn и нажмите на кнопку **Upload** ( ).

6. Выберите метагруппу `CyberTrace_META_GROUP` и нажмите на кнопку **Save and Apply**.



Добавление метагруппы

Шаг 4 (необязательный). Импорт правил Kaspersky CyberTrace Service в RSA NetWitness

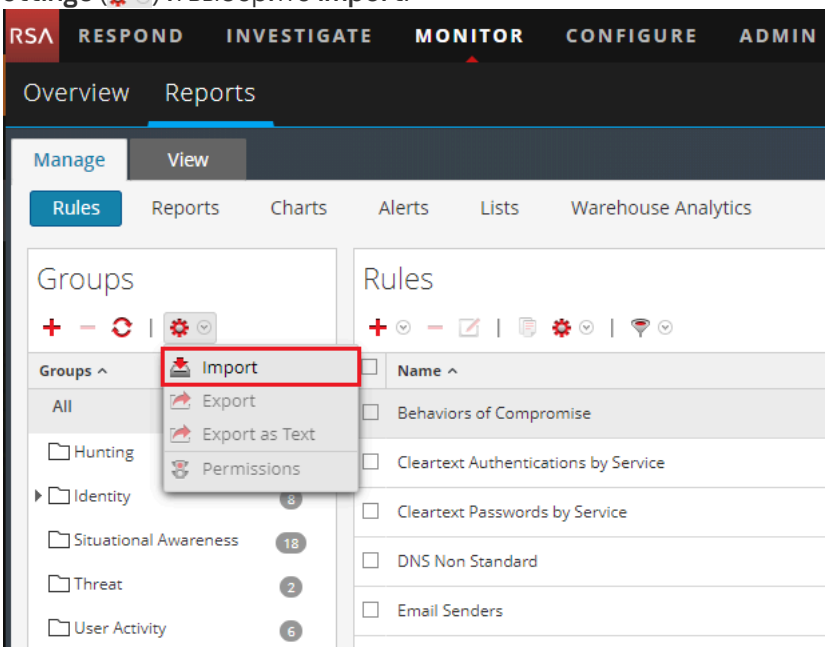
В комплект поставки Kaspersky CyberTrace входит файл CyberTrace_Rules.zip в каталоге `integration/rsa/additional_elements`. Этот файл содержит набор правил, которые можно использовать для создания отчетов, оповещений и информационных панелей.

Чтобы импортировать правила Kaspersky CyberTrace Service в RSA NetWitness, выполните следующие действия:

1. В меню RSA NetWitness выберите **Reports**.

   В RSA NetWitness 11 вместо этого необходимо выбрать **Monitor** → **Reports**.

2. Нажмите на кнопку **Settings** ( ) и выберите **Import**.



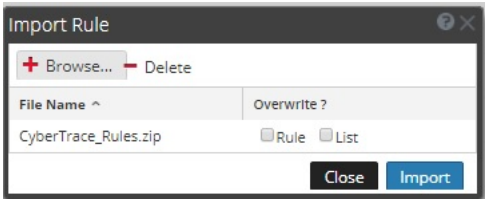
Импорт правил

3. Выберите файл CyberTrace_Rules.zip.

4. В окне **Import Rule** установите флажок **Rule** и флажок **List**.

   Если файл CyberTrace_Rules.zip импортируется впервые, эти флажки можно оставить снятыми.

5. Нажмите на кнопку **Import**.



Импорт правил Kaspersky CyberTrace Service

Правила, импортируемые в RSA NetWitness, перечислены в таблице ниже.

Правило	Описание
CyberTrace Detect Botnet	Выбирает оповещения об обнаружении индикаторов компрометации из службы Kaspersky CyberTrace, имеющие категорию Botnet. Выбираются следующие поля: • url • checksum • ip.src • user.src • event.source

CyberTrace Detect Malware Hash	Выбирает оповещения об обнаружении хешей из службы Kaspersky CyberTrace. Выбираются следующие поля: • virusname • checksum • ip.src • user.src • event.source
CyberTrace Detect Malware IP	Выбирает оповещения об обнаружении IP-адресов из службы Kaspersky CyberTrace. Выбираются следующие поля: • virusname • ip.dst • ip.src • user.src • event.source
CyberTrace Detect Malware URL	Выбирает оповещения об обнаружении URL из службы Kaspersky CyberTrace. Выбираются следующие поля: • virusname • url • ip.src • user.src • event.source
CyberTrace Detect Stat	Выбирает все категории, используемые в процессе обнаружения киберугроз. Выбираются следующие поля: • virusname
CyberTrace Service events	Выбирает служебные оповещения из службы Kaspersky CyberTrace. Выбираются следующие поля: • action • msg
CyberTrace Top 10 IP	Выбирает топ-10 обнаруженных IP-адресов. Выбираются следующие поля: • kl.detected
CyberTrace Top 10 URL	Выбирает топ-10 обнаруженных URL. Выбираются следующие поля: • url
CyberTrace Top 10 Hash	Выбирает топ-10 обнаруженных хешей. Выбираются следующие поля: • checksum
CyberTrace Detected users	Вычисляет количество оповещений об обнаружении индикаторов компрометации на одного пользователя.

Шаг 5 (необязательный). Импорт предварительно настроенного отчета в RSA NetWitness

В этом разделе описывается порядок импорта предварительно настроенного отчета в RSA NetWitness. Порядок создания отчета в ручную приведен в разделе о создании и просмотре отчетов в RSA NetWitness.

Этот шаг требует предварительного выполнения шага Импорт правил Kaspersky CyberTrace Service.

В комплект поставки входит файл CyberTrace_Reports.zip. Этот файл содержит предварительно настроенный отчет — `CyberTrace Report`.

Отчет `CyberTrace Report` содержит следующие данные:

- Статистика обнаружения киберугроз за последние 24 часа
- Статистика по пользователям, сформировавшим события обнаруженных киберугроз за последние 24 часа
- Топ-10 URL, топ-10 IP-адресов топ-10 хешей за последние 24 часа

Этот файл можно импортировать так же, как импортируется файл CyberTrace_Rules.zip (который содержит правила). После импорта отчета необходимо указать источник данных.

Чтобы указать источник данных для отчета «CyberTrace Report», выполните следующие действия:

1. В меню RSA NetWitness выберите **Reports**. (В RSA NetWitness 11 выберите **Monitor** → **Reports**).

   Откроется вкладка **Manage**.

2. Нажмите на кнопку **Reports**.

   Отображается экран **Reports**.

3. На экране **Reports**, в столбце **Actions** нажмите на кнопку **Settings** () для отчета `CyberTrace Report`, затем выберите **Schedule Report**.

   Откроется форма **Schedule Report**.

4. В форме **Schedule Report** укажите следующие данные:

   - Имя расписания
   - Источник данных (база данных из раскрывающегося списка **NetWitness Platform DB**)

     Выберите либо Concentrator, который получает события от Kaspersky CyberTrace Service, либо Log Decoder, в котором хранятся события из Kaspersky CyberTrace Service.

5. Нажмите на кнопку **Schedule**.

Шаг 6 (необязательный). Импорт предварительно настроенных диаграмм и информационной панели в RSA NetWitness

В этом разделе описывается порядок импорта предварительно настроенных диаграмм и информационной панели в RSA NetWitness.

Этот шаг требует предварительного выполнения шага Импорт правил Kaspersky CyberTrace Service.

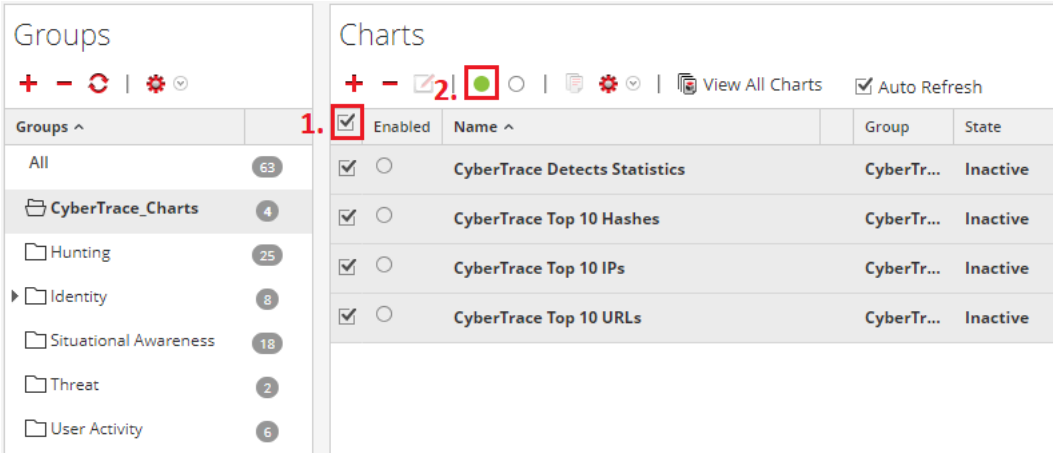
Импорт предварительно настроенных диаграмм

В комплект поставки входит файл CyberTrace_Charts.zip. Файл CyberTrace_Charts.zip содержит предварительно настроенные диаграммы. Эти диаграммы используются в предварительно настроенной информационной панели.

Файл CyberTrace_Charts.zip можно импортировать в том же порядке, что и файл CyberTrace_Rules.zip, содержащий правила.

После импорта файла CyberTrace_Charts.zip укажите источник данных для каждой диаграммы (укажите либо Concentrator, который получает события от Kaspersky CyberTrace Service, либо Log Decoder, в котором хранятся события из Kaspersky CyberTrace Service). Для этого для каждой диаграммы нажмите кнопку **Actions** ( ) и выберите **Edit**. Затем в поле **Data Source** укажите источник данных и нажмите кнопку **Save**.

Кроме того, каждую диаграмму необходимо включить: установите флажки рядом с названиями диаграмм (или установите флажок рядом с заголовком столбца **Enabled**), затем нажмите кнопку **Enable** ( ).



Включение диаграмм

Импорт информационной панели Kaspersky CyberTrace

В комплект поставки также входит файл Kaspersky+CyberTrace.cfg. Этот файл содержит предварительно настроенную информационную панель `Kaspersky CyberTrace`.

Чтобы импортировать файл Kaspersky+ CyberTrace.cfg, необходимо нажать на кнопку **Settings** ( ) в форме **Dashboard** и выбрать **Import**. В форме **Dashboard** появится форма элемента информационной панели. После импорта файла CFG настройте следующие элементы информационной панели: `CyberTrace Detects Statistic`, `CyberTrace Top 10 URL`, `CyberTrace Top 10 Hash` и `CyberTrace Top 10 IP`.

> Приведенная выше инструкция по импорту актуальна для RSA NetWitness версии 10.6. Чтобы импортировать файл Kaspersky CyberTrace.zip в RSA NetWitness версии 11.0, нажмите на кнопку **Import dashboard** ( ).

В RSA NetWitness версии 11.6.0 диаграммы не отображаются по умолчанию. Для настройки отображения диаграмм необходимо нажать на кнопку **Settings** ( ) в каждом окне, затем в окне диаграммы нажать на кнопку **Обзор** и выбрать требуемую диаграмму.

Шаг 7. Проверка работоспособности (RSA NetWitness)

После настройки Kaspersky CyberTrace и RSA NetWitness можно протестировать их работу.

> Прежде чем редактировать какие-либо правила фильтрации в конфигурационном файле Feed Utility, следует обязательно выполнить проверку работоспособности.

Чтобы проверить правильность интеграции Kaspersky CyberTrace с RSA NetWitness, выполните следующие действия:

1. Настройте Log Scanner для отправки событий на IP-адрес и порт, которые прослушивает Kaspersky CyberTrace Service.

   Для этого в элементе `Connection` конфигурационного файла Log Scanner укажите IP-адрес и порт, заданные для исходящих событий на странице **Параметры → Служба** в веб-интерфейсе Kaspersky CyberTrace.

2. Отправьте файл `kl_verification_test_cef.txt` из каталога verification в Kaspersky CyberTrace Service с помощью Log Scanner.

   Для этого выполните следующую команду:

   В ОС Linux: `./log_scanner -p ../verification/kl_verification_test_cef.txt`

   В ОС Windows: `log_scanner.exe -p ..\verification\kl_verification_test_cef.txt`

   > Не указывайте в этой команде флаг `-r` — отправлять результаты проверки в SIEM-систему с использованием параметров для исходящих событий, указанных на вкладке **Параметры → Служба** в Kaspersky CyberTrace.

3. Убедитесь, что полученные результаты проверки соответствуют следующей таблице.

   Результаты проверки можно просматривать так же, как и при просмотре событий Kaspersky CyberTrace Service в RSA NetWitness.

Результаты проверки работоспособности

Результаты проверки работоспособности зависят от используемых потоков данных об угрозах. Результаты проверки работоспособности приведены в следующей таблице.

Результаты проверки работоспособности

Используемый поток данных об угрозах	Обнаруженные объекты
Malicious URL Data Feed	http://fakess123.nu http://badb86360457963b90faac9ae17578ed.com
Phishing URL Data Feed	http://fakess123ap.nu http://e77716a952f640b42e4371759a661663.com
Botnet C&C URL Data Feed	http://fakess123bn.nu http://a7396d61caffe18a4cffbb3b428c9b60.com
IP Reputation Data Feed	192.0.2.0 192.0.2.3
Malicious Hash Data Feed	FEAF2058298C1E174C2B79AFFC7CF4DF 44D88612FEA8A8F36DE82E1278ABB02F (EICAR Standard Anti-Virus Test File) C912705B4BBB14EC7E78FA8B370532C9
Mobile Malicious Hash Data Feed	60300A92E1D0A55C7FDD360EE40A9DC1
Mobile Botnet C&C URL Data Feed	001F6251169E6916C455495050A3FB8D (хеш MD5) sdfed7233dsfg93acvbhl.su/steallallsms.php (маска URL)
Ransomware URL Data Feed	http://fakess123r.nu http://fa7830b4811fbef1b187913665e6733c.com
APT URL Data Feed	http://b046f5b25458638f6705d53539c79f62.com
APT Hash Data Feed	7A2E65A0F70EE0615EC0CA34240CF082

APT IP Data Feed	192.0.2.4
IoT URL Data Feed	http://e593461621ee0f9134c632d00bf108fd.com/.i
Demo Botnet C&C URL Data Feed	http://5a015004f9fc05290d87e86d69c4b237.com http://fakess123bn.nu
Demo IP Reputation Data Feed	192.0.2.1 192.0.2.3
Demo Malicious Hash Data Feed	776735A8CA96DB15B422879DA599F474 FEAF2058298C1E174C2B79AFFC7CF4DF 44D88612FEA8A8F36DE82E1278ABB02F
ICS Hash Data Feed	7A8F30B40C6564EFF95E678F7C43346C

Интеграция с LogRhythm

В этой главе описывается порядок интеграции Kaspersky CyberTrace с LogRhythm.

Действия, описываемые в этих разделах, необходимо выполнять в LogRhythm Console под учетной записью пользователя с правами администратора.

Порядок интеграции LogRhythm с Kaspersky CyberTrace:

1. Добавление типа источника журналов Kaspersky CyberTrace в LogRhythm.
2. Импорт файлов с правилами Kaspersky CyberTrace.
3. Дополнительно можно добавить события Kaspersky CyberTrace в LogRhythm.
4. Дополнительно можно добавить правила Kaspersky CyberTrace в LogRhythm.
5. Добавьте политику Kaspersky CyberTrace в LogRhythm.
6. Примите источник журнала Kaspersky CyberTrace в LogRhythm.
7. Настройте пересылку журналов в Kaspersky CyberTrace на стороне LogRhythm.
8. Выполните проверку работоспособности.
9. Создайте оповещения о входящих служебных событиях Kaspersky CyberTrace (необязательно).
10. Настройте отображение событий оповещений в LogRhythm (необязательно).

Шаг 1. Добавление пользовательского типа источника журналов

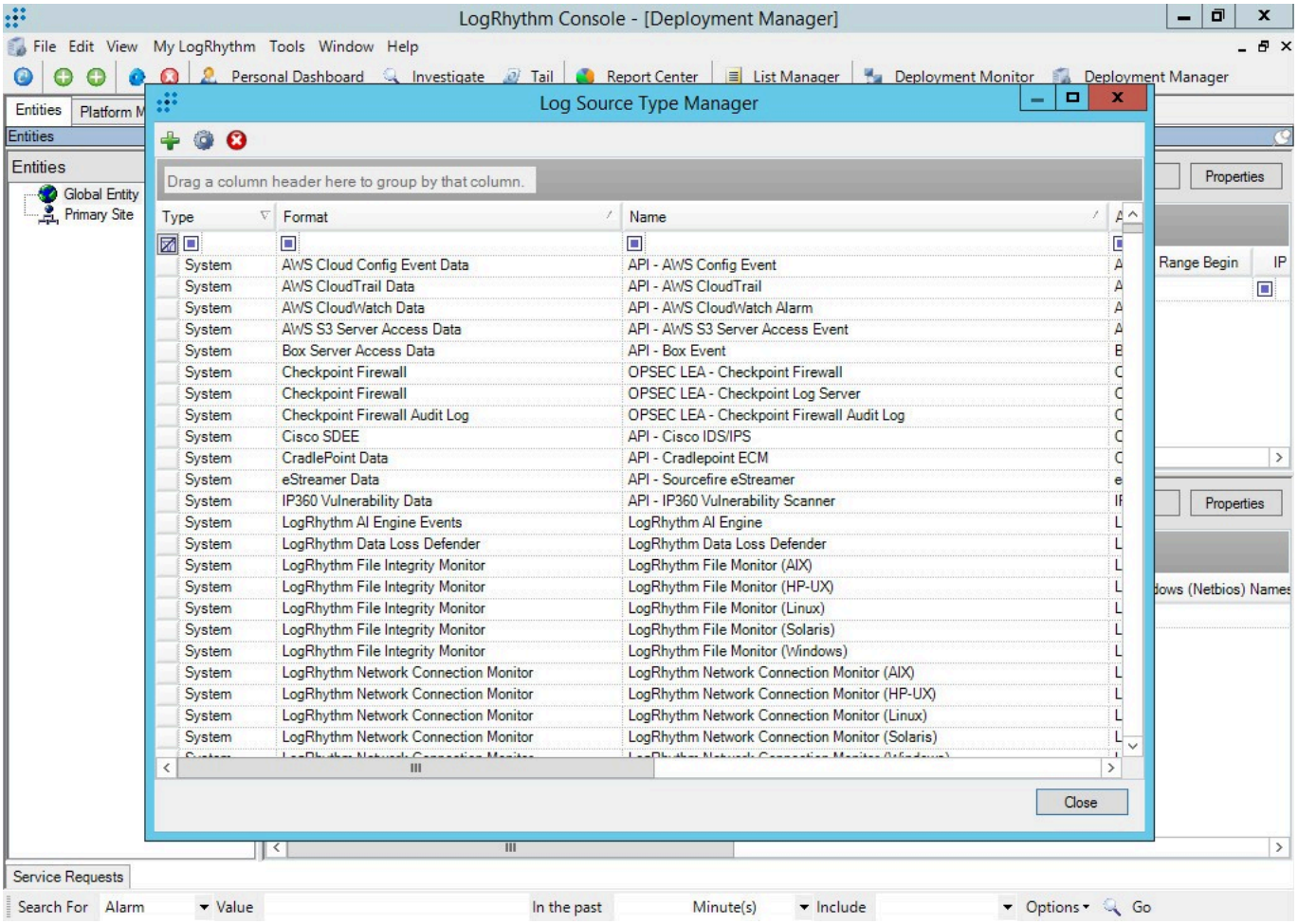
В этом разделе описывается, порядок добавления в LogRhythm типа источника журнала Kaspersky CyberTrace.

Чтобы добавить тип источника журнала Kaspersky CyberTrace в LogRhythm, выполните следующие действия:

1. Запустите LogRhythm Console.

2. Выберите **Deployment Manager** → **Tools** → **Knowledge** → **Log Source Type Manager**.

   Откроется окно **Log Source Type Manager**.

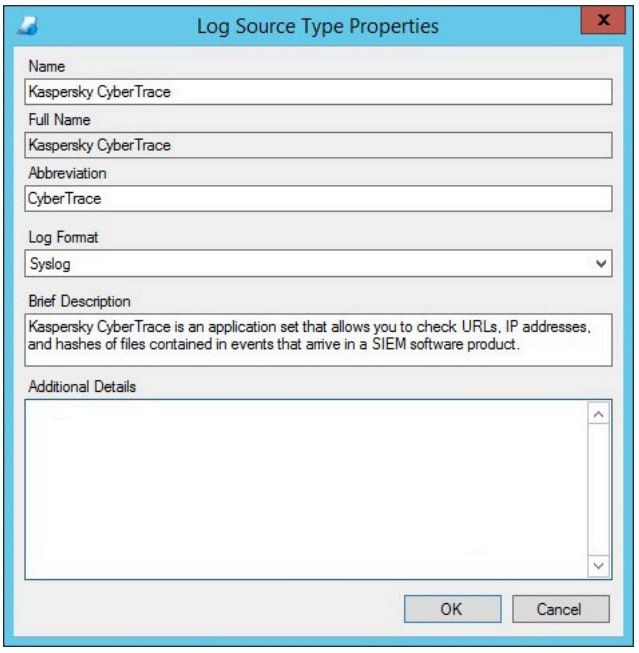


Окно **Log Source Type Manager**

3. Нажмите на кнопку **New** ( ).

4. В открывшемся окне **Log Source Type Properties** введите следующие данные:

Поле	Данные
Name	Kaspersky CyberTrace
Full name	Kaspersky CyberTrace
Abbreviation	CyberTrace
Log Format	Syslog
Brief Description	Kaspersky CyberTrace is an application set that allows you to check URLs, IP addresses, and hashes of files contained in events that arrive in a SIEM.



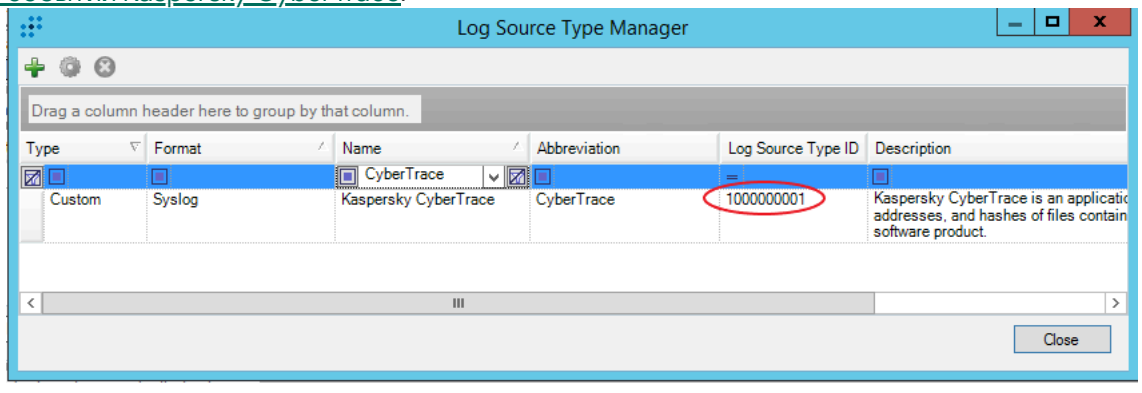
Окно **Log Source Type Properties**

Также рекомендуется указать имя источника в поле **Имя**, как описано в таблице выше. В противном случае импорт правил и событий Kaspersky CyberTrace будет выполнен некорректно. В этом случае необходимо добавить события Kaspersky CyberTrace и соответствующие правила MPE вручную, как описано на шаге 3 и шаге 4 (обязательно следует указать имя источника журналов, похожее на имя, ранее введенное в окне **Log Source Type Properties**).

5. Нажмите на кнопку **OK**.

   Новый тип источника журналов появится в окне **Log Source Type Manager**.

6. Запишите или запомните значение в столбце **Log Source Type ID**. Он понадобится на шаге 2 для импорта правил и событий Kaspersky CyberTrace.



Тип источника журналов Kaspersky CyberTrace

Шаг 2. Импорт правил и событий Kaspersky CyberTrace

В этом разделе описывается порядок импорта в LogRhythm файлов, содержащих правила и события Kaspersky CyberTrace.

Если по какой-либо причине импорт не удается, можно настроить добавление событий Kaspersky CyberTrace и правил Kaspersky CyberTrace вручную.

Чтобы импортировать в LogRhythm файлы с правилами Kaspersky CyberTrace, выполните следующие действия:

1. Для каждого файла формата `mperule_%event_name%.xml` из каталога `integration/logrhythm/events/` выполните следующие действия:

   a. Откройте файл в текстовом редакторе.

   b. Замените значения элементов `MPERuleToMST > MsgSourceTypeID` и `MsgSourceType > MsgSourceTypeID` идентификатором типа источника журналов из предыдущего шага.

   Например, `<MsgSourceTypeID>1000000001</MsgSourceTypeID>` следует заменить на `<MsgSourceTypeID>%CYBERTRACE_ID%</MsgSourceTypeID>`, где `%CYBERTRACE_ID%` — идентификатор типа источника журнала Kaspersky CyberTrace.

   c. Сохраните файл.

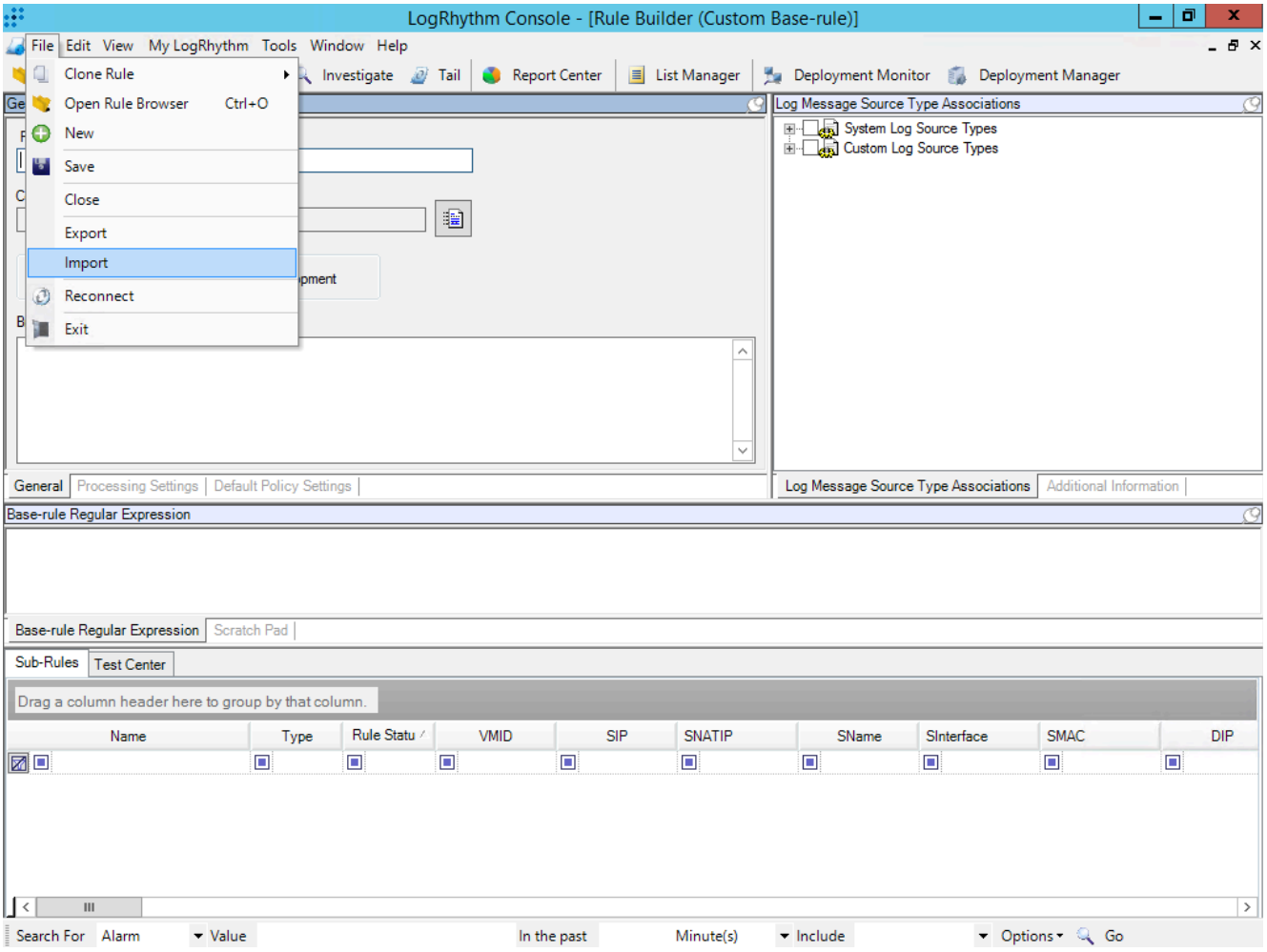
2. Откройте LogRhythm Console.

3. Выберите **Deployment Manager** → **Tools** → **Knowledge** → **MPE Rule Builder**.

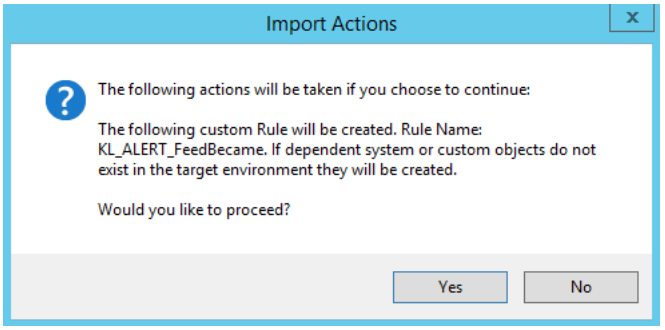
   Откроется форма **Rule Builder**.

4. Для каждого файла, отредактированного на шаге 1 выше, выполните следующие действия:

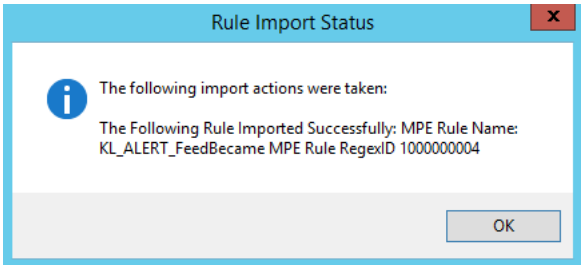
a. Выберите **File** → **Import**.



b. В окне **Import Actions** нажмите на кнопку **Yes**.



Если импорт завершится успешно, откроется окно **Rule Import Status**.



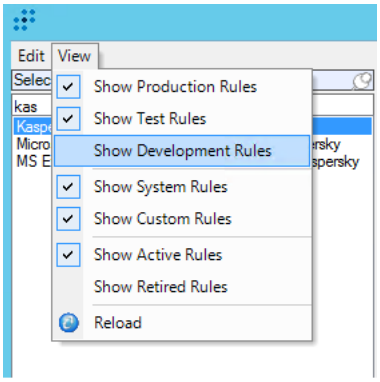
c. На панели инструментов формы **Rule Builder** нажмите на кнопку **Open rule library** ( ).

Откроется окно **Rule Browser**.

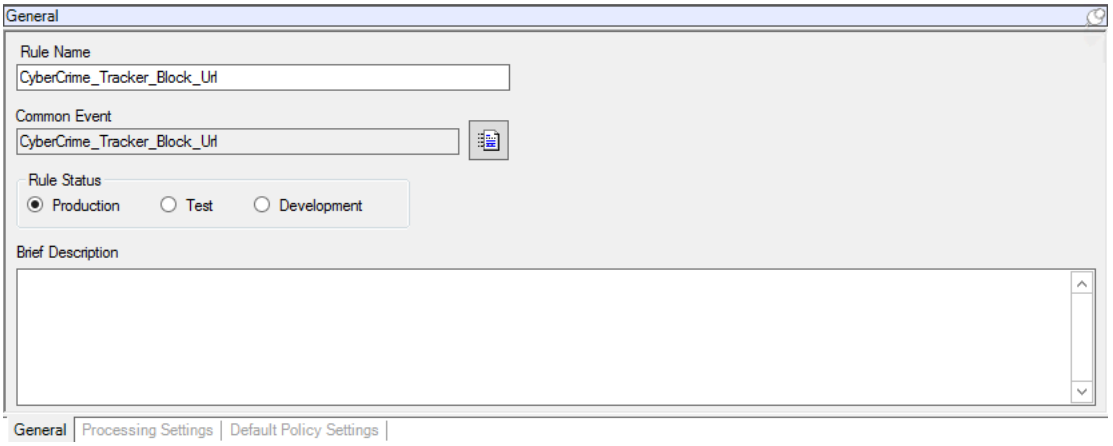
d. Дважды нажмите на событие, которое было импортировано на шаге b.

Откроется окно с настройками правила.

Обратите внимание, что импортированное правило поступает в LogRhythm в статусе `Development` и может не отображаться в списке всех правил. Отображение можно настроить в окне **Rule Browser**, которое открывается при выборе **View** → **Show Development Rules**.



e. В открывшемся окне настроек **General** в разделе **Rule Status** выберите **Production** или **Test**.



f. Нажмите на кнопку **Save**.

Соответствующие общие события и правила MPE добавляются в LogRhythm для всех событий. Полный список событий описан в разделе о добавлении событий Kaspersky CyberTrace. Полный список правил MPE и их настройки описаны в разделе о добавлении правил Kaspersky CyberTrace.

Некоторые из импортированных событий Kaspersky CyberTrace могут иметь низкий рейтинг риска по классификации LogRhythm. В зависимости от настройки фильтров LogRhythm может игнорировать такие события. Проверьте классификацию и убедитесь, что рейтинг риска импортированных событий позволяет LogRhythm правильно их принимать и обрабатывать.

Шаг 3 (необязательный). Добавление событий Kaspersky CyberTrace

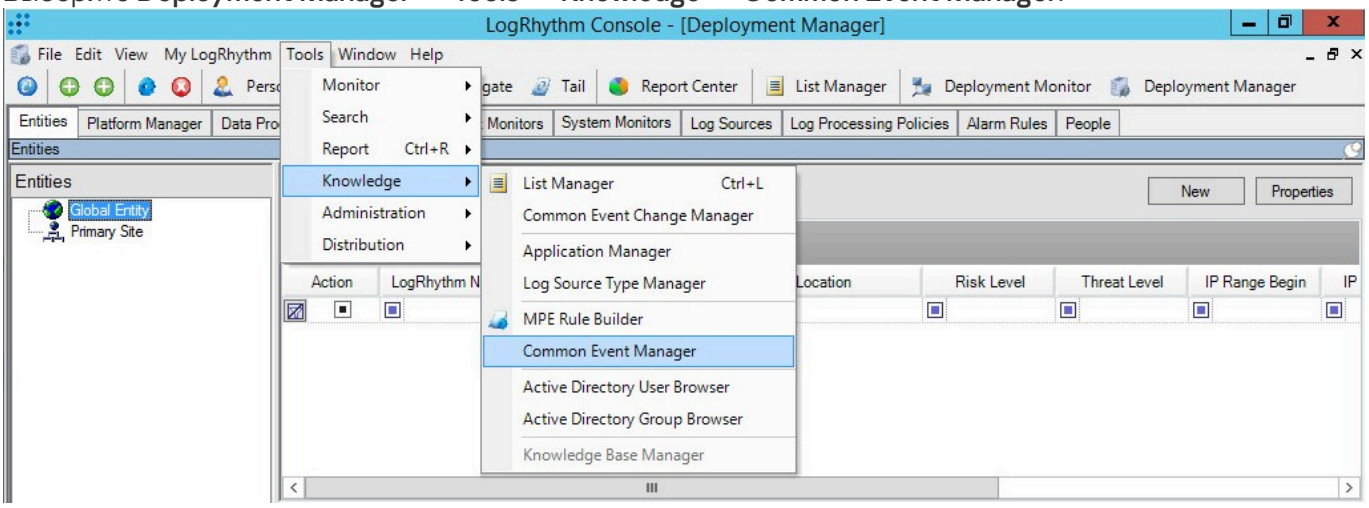
В этом разделе описывается порядок добавления оповещений Kaspersky CyberTrace в LogRhythm вручную.

Пропустите этот шаг, если импорт правил и оповещений Kaspersky CyberTrace выполнен успешно.

Чтобы добавить оповещения Kaspersky CyberTrace в LogRhythm, выполните следующие действия:

1. Запустите LogRhythm Console.

2. Выберите **Deployment Manager** → **Tools** → **Knowledge** → **Common Event Manager**.



Пункт меню **Common Event Manager**

Откроется окно **Common Event Manager**.

3. Добавьте оповещение, указанные в таблицах ниже. Если используются не все коммерческие потоки данных и потоки данных «OSINT feed», некоторые оповещения могут не понадобиться.

   - Оповещения классификации «`Security : Compromise`»

Оповещение	Описание
KL_APT_Hash_MD5	Kaspersky CyberTrace обнаруживает хеш вредоносного файла, используемого в APT-кампании.
KL_APT_Hash_SHA1	Kaspersky CyberTrace обнаруживает хеш вредоносного файла, используемого в APT-кампании.
KL_APT_Hash_SHA256	Kaspersky CyberTrace обнаруживает хеш вредоносного файла, используемого в APT-кампании.
KL_APT_IP	Kaspersky CyberTrace обнаруживает IP-адрес, используемый в APT-кампании.
KL_APT_URL	Kaspersky CyberTrace обнаруживает URL, используемый в APT-кампании.
KL_BotnetCnC_Hash_MD5	Kaspersky CyberTrace обнаруживает хеш ботнета.
KL_BotnetCnC_Hash_SHA1	Kaspersky CyberTrace обнаруживает хеш ботнета.
KL_BotnetCnC_Hash_SHA256	Kaspersky CyberTrace обнаруживает хеш ботнета.
KL_BotnetCnC_URL	Kaspersky CyberTrace обнаруживает URL командного сервера (C&C) ботнета.
KL_ICS_Hash_MD5	Kaspersky CyberTrace обнаруживает хеш ICS.
KL_ICS_Hash_SHA1	Kaspersky CyberTrace обнаруживает хеш ICS.
KL_ICS_Hash_SHA256	Kaspersky CyberTrace обнаруживает хеш ICS.
KL_InternalTI_URL	URL списка пользовательских сведений о киберугрозах Kaspersky CyberTrace.
KL_InternalTI_IP	IP-адрес списка пользовательских сведений о киберугрозах Kaspersky CyberTrace.
KL_InternalTI_Hash_MD5	Хеш списка пользовательских сведений о киберугрозах Kaspersky CyberTrace.
KL_InternalTI_Hash_SHA1	Хеш списка пользовательских сведений о киберугрозах Kaspersky CyberTrace.
KL_InternalTI_Hash_SHA256	Хеш списка пользовательских сведений о киберугрозах Kaspersky CyberTrace.
KL_IoT_Hash_MD5	Kaspersky CyberTrace обнаруживает хеш IoT.

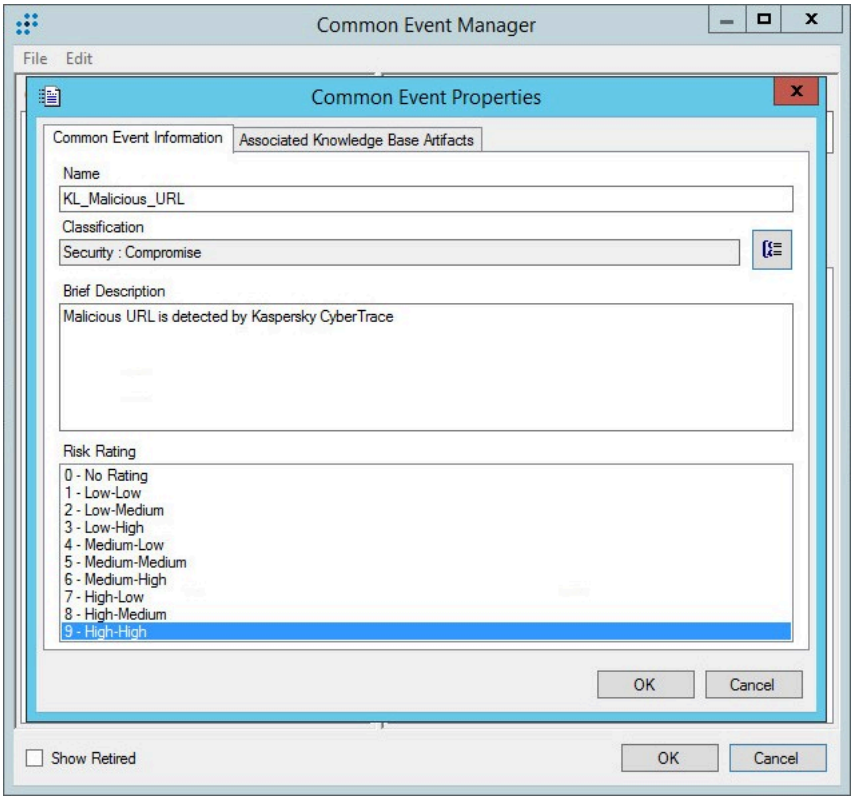
KL_IoT_Hash_SHA1	Kaspersky CyberTrace обнаруживает хеш IoT.
KL_IoT_Hash_SHA256	Kaspersky CyberTrace обнаруживает хеш IoT.
KL_IoT_URL	Kaspersky CyberTrace обнаруживает URL, заражающий устройства с поддержкой интернета вещей (IoT).
KL_IP_Reputation	Kaspersky CyberTrace обнаруживает вредоносный IP-адрес.
KL_IP_Reputation_Hash_MD5	Kaspersky CyberTrace обнаруживает хеш файла, размещенного на вредоносном IP-адресе.
KL_IP_Reputation_Hash_SHA1	Kaspersky CyberTrace обнаруживает хеш файла, размещенного на вредоносном IP-адресе.
KL_IP_Reputation_Hash_SHA256	Kaspersky CyberTrace обнаруживает хеш файла, размещенного на вредоносном IP-адресе.
KL_Malicious_URL	Kaspersky CyberTrace обнаруживает вредоносный URL.
KL_Malicious_URL_Hash_MD5	Kaspersky CyberTrace обнаруживает хеш файла, размещенного на вредоносном URL.
KL_Malicious_URL_Hash_SHA1	Kaspersky CyberTrace обнаруживает хеш файла, размещенного на вредоносном URL.
KL_Malicious_URL_Hash_SHA256	Kaspersky CyberTrace обнаруживает хеш файла, размещенного на вредоносном URL.
KL_Malicious_Hash_MD5	Kaspersky CyberTrace обнаруживает вредоносный хеш.
KL_Malicious_Hash_SHA1	Kaspersky CyberTrace обнаруживает вредоносный хеш.
KL_Malicious_Hash_SHA256	Kaspersky CyberTrace обнаруживает вредоносный хеш.
KL_Mobile_Malicious_Hash_MD5	Kaspersky CyberTrace обнаруживает вредоносный мобильный хеш.
KL_Mobile_Malicious_Hash_SHA1	Kaspersky CyberTrace обнаруживает вредоносный мобильный хеш.
KL_Mobile_Malicious_Hash_SHA256	Kaspersky CyberTrace обнаруживает вредоносный мобильный хеш.
KL_Mobile_BotnetCnC_Hash_MD5	Kaspersky CyberTrace обнаруживает хеш командного сервера (C&C) мобильного ботнета.
KL_Mobile_BotnetCnC_Hash_SHA1	Kaspersky CyberTrace обнаруживает хеш командного сервера (C&C) мобильного ботнета.
KL_Mobile_BotnetCnC_Hash_SHA256	Kaspersky CyberTrace обнаруживает хеш командного сервера (C&C) мобильного ботнета.
KL_Mobile_BotnetCnC_URL	Kaspersky CyberTrace обнаруживает URL командного сервера (C&C) мобильного ботнета.
KL_Phishing_URL	Kaspersky CyberTrace обнаруживает фишинговый URL.
KL_Ransomware_URL	Kaspersky CyberTrace обнаруживает URL, на котором размещена программа-вымогатель.
KL_Ransomware_URL_Hash_MD5	Kaspersky CyberTrace обнаруживает хеш программы-вымогателя.
KL_Ransomware_URL_Hash_SHA1	Kaspersky CyberTrace обнаруживает хеш программы-вымогателя.
KL_Ransomware_URL_Hash_SHA256	Kaspersky CyberTrace обнаруживает хеш программы-вымогателя.
AbuseCh_Feodo_Block_IP	Kaspersky CyberTrace обнаруживает IP-адрес из потока данных об угрозах Abuse.Ch_Feodo_Block_IP.
AbuseCh_Ransomware_Block_URL	Kaspersky CyberTrace обнаруживает URL из потока данных об угрозах Abuse.Ch_Ransomware_Block_URL.
AbuseCh_Ransomware_Block_Domain	Kaspersky CyberTrace обнаруживает домен из потока данных об угрозах Abuse.Ch_Ransomware_Block_Domain.
AbuseCh_Ransomware_Block_IP	Kaspersky CyberTrace обнаруживает IP-адрес из потока данных об угрозах Abuse.Ch_Ransomware_Block_IP.
AbuseCh_Ransomware_Common_URL	Kaspersky CyberTrace обнаруживает URL из потока данных об угрозах Abuse.Ch_Ransomware_Common_URL.
AbuseCh_SSL_Certificate_Block_IP	Kaspersky CyberTrace обнаруживает IP-адрес из потока данных об угрозах AbuseCh_SSL_Certificate_Block_IP.
AbuseCh_SSL_Certificate_Hash_SHA1	Kaspersky CyberTrace обнаруживает хеш из потока данных об угрозах AbuseCh_SSL_Certificate_Hash_SHA1.
BlocklistDe_Block_IP	Kaspersky CyberTrace обнаруживает IP-адрес из потока данных об угрозах BlocklistDe_Block_IP.
CyberCrime_Tracker_Block_Url	Kaspersky CyberTrace обнаруживает URL из потока данных об угрозах CyberCrime_Tracker_Block_Url.

EmergingThreats_Block_IP	Kaspersky CyberTrace обнаруживает IP-адрес из потока данных об угрозах EmergingThreats_Block_IP.
EmergingThreats_Compromised_IP	Kaspersky CyberTrace обнаруживает IP-адрес из потока данных об угрозах EmergingThreats_Compromised_IP.

- Служебные оповещения:

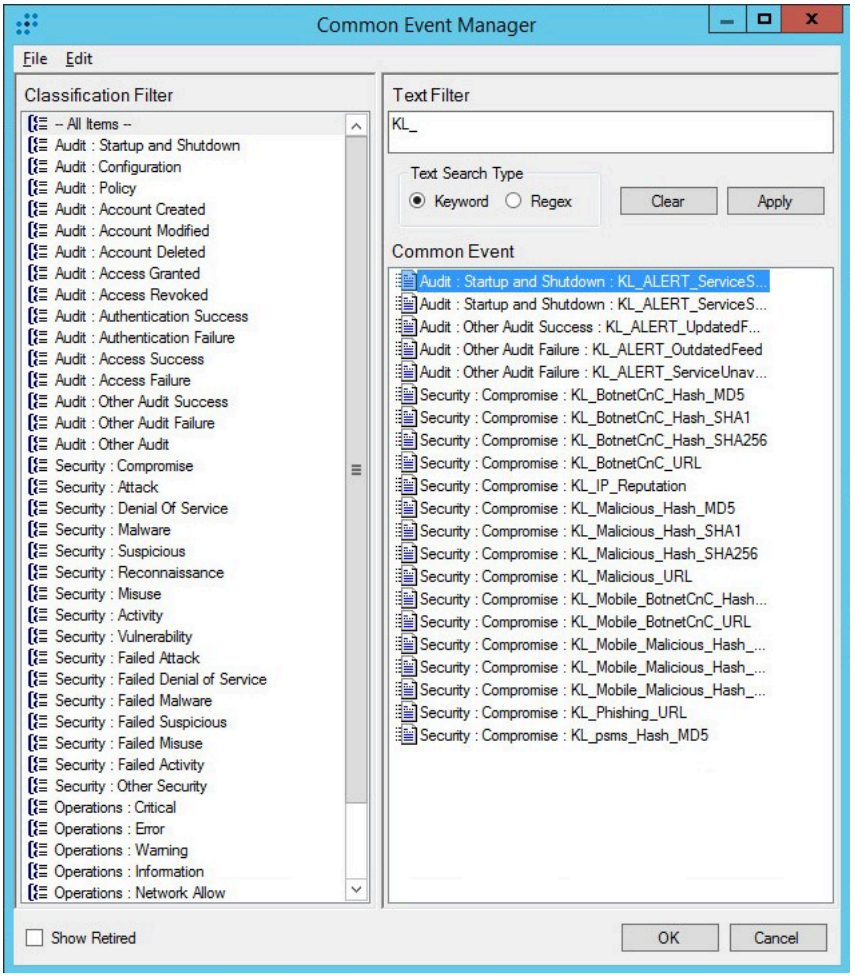
Оповещение	Описание	Классификация
KL_ALERT_ConfigurationUpdated	Это оповещение генерируется, если Kaspersky CyberTrace Service перезагрузил конфигурационный файл.	Audit : Configuration
KL_ALERT_FeedBecameAvailable	Это оповещение генерируется, если стал доступен поток данных об угрозах, который можно использовать с текущим сертификатом.	Audit : Other Audit Success
KL_ALERT_FeedBecameUnavailable	Это оповещение генерируется, если стал недоступен поток данных об угрозах, который используется с текущим сертификатом.	Audit : Other Audit Failure
KL_ALERT_OutdatedFeed	Это оповещение генерируется, если поток данных об угрозах не обновлялся в течение заданного периода.	Audit : Other Audit Failure
KL_ALERT_ServiceUnavailable	Это оповещение генерируется при аварийном завершении или зависании службы Kaspersky CyberTrace.	Audit : Other Audit Failure
KL_ALERT_ServiceStopped	Это оповещение генерируется при успешной остановке Kaspersky CyberTrace Service.	Audit : Startup and Shutdown
KL_ALERT_ServiceStarted	Это оповещение генерируется при успешном запуске Kaspersky CyberTrace Service.	Audit : Startup and Shutdown
KL_ALERT_UpdatedFeed	Это оповещение генерируется при обновлении и загрузке потока данных об угрозах в Kaspersky CyberTrace Service.	Audit : Other Audit Success
KL_ALERT_FailedToUpdateFeed	Это оповещение генерируется, когда Kaspersky CyberTrace Service не удается загрузить новый поток данных (например, из-за ограничения на количество индикаторов, налагаемого лицензионным ключом), и продолжает использоваться старый поток данных:	Audit : Other Audit Failure
KL_ALERT_LicenseExpires	Это оповещение генерируется для информирования о том, что используемый лицензионный ключ истечет менее чем через 30 дней.	Audit : Policy
KL_ALERT_LicenseExpired	Это оповещение генерируется, когда истекает срок действия лицензионного ключа.	Audit : Policy
KL_ALERT_EPSLimitExceeded	Это оповещение генерируется, когда оказывается превышен лимит на количество обрабатываемых событий в секунду (EPS), установленный лицензионным ключом или уровнем лицензирования.	Audit : Policy
KL_ALERT_EPSHardLimit	Это оповещение генерируется, когда Kaspersky CyberTrace Service ограничивает количество обрабатываемых событий в секунду (EPS) до максимального количества событий для текущего лицензионного ключа или уровня лицензирования. Лимит действует независимо от количества входящих событий. Это ограничение действует независимо от количества входящих событий.	Audit : Policy
KL_ALERT_LicenseChanged	Это оповещение генерируется, когда Kaspersky CyberTrace начинает использовать другой лицензионный ключ или другой уровень лицензирования.	Audit : Configuration
KL_ALERT_RetroScanError	Это оповещение генерируется при отказе задачи ретроспективного сканирования.	Audit : Other Audit Failure
KL_ALERT_RetroScanCompleted	Это оповещение генерируется при успешном выполнении задачи ретроспективного сканирования.	Audit : Other Audit Success
KL_ALERT_RetroScanStorageExceeded	Это оповещение генерируется при превышении ограничения на размер сохраняемых событий.	Audit : Policy
KL_ALERT_IndicatorsStoreLimitExceeded	Это оповещение генерируется при превышении ограничения на размер сохраняемых индикаторов.	Audit : Policy
KL_ALERT_IndicatorsStoreHardLimit	Это оповещение генерируется, когда Kaspersky CyberTrace ограничивает добавление и обновление индикаторов.	Audit : Policy
KL_ALERT_FreeSpaceEnds	Это оповещение генерируется, когда на диске остается мало свободного места.	Audit : Policy

Оповещения могут содержать поля контекста, как описано в разделе об оповещениях Kaspersky CyberTrace.



Окно **Common Event Properties**

После добавления оповещений окно **Common Event Manager** должно содержать оповещения, как показано на рисунке ниже.



Добавленные оповещения

Шаг 4 (необязательный). Добавление правил Kaspersky CyberTrace

В этом разделе описывается порядок добавления правил Kaspersky CyberTrace в LogRhythm вручную.

Пропустите этот шаг, если импорт правил и событий Kaspersky CyberTrace выполнен успешно.

Чтобы добавить правила Kaspersky CyberTrace в LogRhythm, выполните следующие действия:

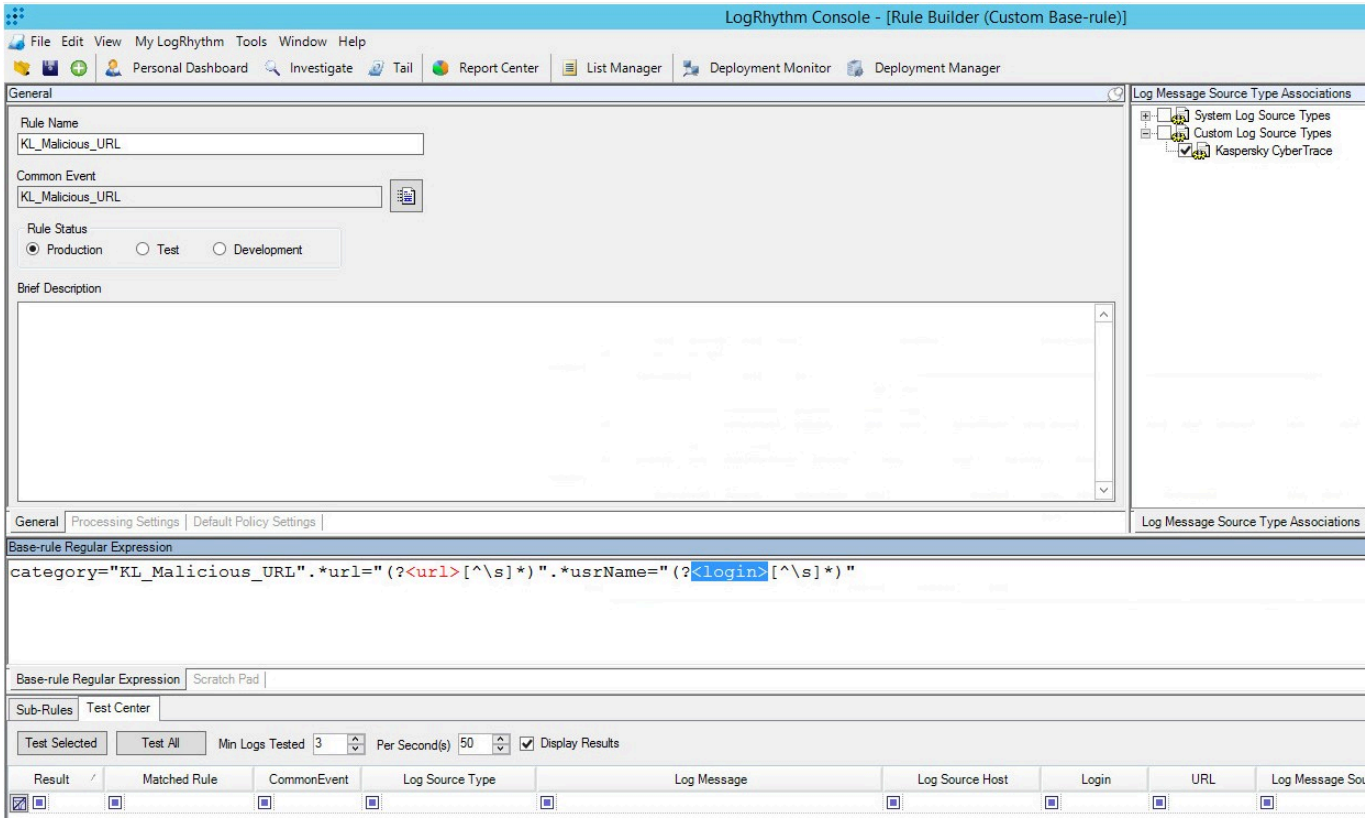
1. Запустите LogRhythm Console.
2. Выберите **Deployment Manager** → **Tools** → **Knowledge** → **MPE Rule Builder**.
   Откроется форма **Rule Builder**.
3. Для каждого события добавьте правило, для этого нажмите на кнопку **Create a new rule** ( ).
   Для каждого правила выполните следующие действия:
   - В разделе **General** нажмите на кнопку рядом с полем **Common Event** и выберите требуемое событие.
     Событие отображается в поле.

- В разделе **Log Message Source Type Associations** укажите `Kaspersky CyberTrace` в качестве типа источника журнала.

- Чтобы установить статус правила, выберите вариант **Production** или **Test**.

  При создании регулярных выражений (в разделе **Base-rule Regular Expressions**) следуйте инструкции, приведенной в разделе справки LogRhythm «Use MPE Rule Builder - Parsing Fields and Tags».

  Рекомендуется использовать регулярные выражения, приведенные в таблице ниже.



Форма конструктора правил

В следующем списке приведены регулярные выражения для каждого события. Если требуется использовать другие регулярные выражения, для проверки собственных регулярных выражений следует воспользоваться примерами событий из второго столбца таблицы.

- AbuseCh_Feodo_Block_IP

Регулярное выражение	Пример события для проверки регулярных выражений
`category=AbuseCh_Feodo_Block_IP.*ip=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=AbuseCh_Feodo_Block_IP matchedIndicator=103.11.83.52 url=- src=- ip=103.11.83.52 md5=- sha1=- sha256=- usrName=VerifTestUserName ip=103.11.83.52 source=https://feodotracker.abuse.ch/downloads/ipblocklist.txt`

- AbuseCh_Ransomware_Block_URL

Регулярное выражение	Пример события для проверки регулярных выражений
`category=AbuseCh_Ransomware_Block_URL.*url=(?<url>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=AbuseCh_Ransomware_Block_URL matchedIndicator=00005ik.rcomhost.com/7fg3g url=00005ik.rcomhost.com/7fg3g src=- ip=- md5=- sha1=- sha256=- usrName=- source=https://ransomwaretracker.abuse.ch/downloads/RW_URLBL.txt url=00005ik.rcomhost.com/7fg3g`

- AbuseCh_Ransomware_Block_Domain

Регулярное выражение	Пример события для проверки регулярных выражений
`category=AbuseCh_Ransomware_Block_Domain.*url=(?<url>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=AbuseCh_Ransomware_Block_Domain matchedIndicator=pagaldaily.com url=pagaldaily.com src=- ip=- md5=- sha1=- sha256=- usrName=- domain=pagaldaily.com source=https://ransomwaretracker.abuse.ch/downloads/RW_DOMBL.txt`

- AbuseCh_Ransomware_Block_IP

Регулярное выражение	Пример события для проверки регулярных выражений
`category=AbuseCh_Ransomware_Block_IP.*ip=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=AbuseCh_Ransomware_Block_IP matchedIndicator=83.217.11.193 url=- src=- ip=83.217.11.193 md5=- sha1=- sha256=- usrName=VerifTestUserName ip=83.217.11.193 source=https://ransomwaretracker.abuse.ch/downloads/RW_IPBL.txt`

- AbuseCh_Ransomware_Common_URL

Регулярное выражение	Пример события для проверки регулярных выражений
`category=AbuseCh_Ransomware_Common_URL.*url=(?<url>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=AbuseCh_Ransomware_Common_URL matchedIndicator=83.217.11.193/linuxsucks.php url=83.217.11.193/linuxsucks.php src=- ip=- md5=- sha1=- sha256=- usrName=- ASN=199669 IPList=[{ ip=83.217.11.193}] country=RU domain=83.217.11.193 first_seen=12.08.2018 00:46 malware=Locky registar= source=https://ransomwaretracker.abuse.ch/feeds/csv/ status=offline threat=C2 url=83.217.11.193/linuxsucks.php`

- AbuseCh_SSL_Certificate_Block_IP

Регулярное выражение	Пример события для проверки регулярных выражений
`category=AbuseCh_SSL_Certificate_Block_IP.*ip=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=AbuseCh_SSL_Certificate_Block_IP matchedIndicator=83.217.11.193 url=- src=- ip=83.217.11.193 md5=- sha1=- sha256=- usrName=VerifTestUserName ip=83.217.11.193 source=https://sslbl.abuse.ch/blacklist/sslblacklist.csv`

- AbuseCh_SSL_Certificate_Hash_SHA1

Регулярное выражение	Пример события для проверки регулярных выражений
`category=AbuseCh_SSL_Certificate_Hash_SHA1.*sha1=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=AbuseCh_SSL_Certificate_Hash_SHA1 matchedIndicator=3395856ce81f2b7382dee72602f798b642f14140 url=- src=- ip=- md5=- sha1=3395856ce81f2b7382dee72602f798b642f14140 sha256=- usrName=VerifTestUserName MD5=86255ec982e822f6b57855d3866618ae data_added=2015-09-22`

- BlocklistDe_Block_IP

Регулярное выражение	Пример события для проверки регулярных выражений
`category=BlocklistDe_Block_IP.*ip=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=BlocklistDe_Block_IP matchedIndicator=83.217.11.193 url=- src=- ip=83.217.11.193 md5=- sha1=- sha256=- usrName=VerifTestUserName ip=83.217.11.193`

- CyberCrime_Tracker_Block_Url

Регулярное выражение	Пример события для проверки регулярных выражений
`category=CyberCrime_Tracker_Block_Url.*url=(?<url>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=CyberCrime_Tracker_Block_Url matchedIndicator=83.217.11.193/linuxsucks.php url=83.217.11.193/linuxsucks.php src=- ip=- md5=- sha1=- sha256=- usrName=- ASN=199669 IPList=[{ ip=83.217.11.193}] country=RU domain=83.217.11.193 first_seen=12.08.2018 00:46 malware=Locky status=offline threat=C2 url=83.217.11.193/linuxsucks.php`

- EmergingThreats_Block_IP

Регулярное выражение	Пример события для проверки регулярных выражений
`category=EmergingThreats_Block_IP.*ip=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=EmergingThreats_Block_IP matchedIndicator=101.200.81.187 url=- src=- ip=101.200.81.187 md5=- sha1=- sha256=- usrName=VerifTestUserName ip=101.200.81.187 source=https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt`

- EmergingThreats_Compromised_IP

Регулярное выражение	Пример события для проверки регулярных выражений
`category=EmergingThreats_Compromised_IP.*ip=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=EmergingThreats_Compromised_IP matchedIndicator=100.24.121.249 url=- src=- ip=100.24.121.249 md5=- sha1=- sha256=- usrName=VerifTestUserName ip=100.24.121.249 source=https://rules.emergingthreats.net/blockrules/compromised-ips.txt`

- KL_ALERT_FeedBecameAvailable

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_FeedBecameAvailable.*feed=(?<object>[^\s]*)`	`May 2 16:41:40 alert=KL_ALERT_FeedBecameAvailable feed=Botnet_CnC_URL_Data_Feed.json`

- KL_ALERT_FeedBecameUnavailable

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_FeedBecameUnavailable.*feed=(?<object>[^\s]*)`	`May 2 16:41:40 alert=KL_ALERT_FeedBecameUnavailable feed=Botnet_CnC_URL_Data_Feed.json`

- KL_ALERT_OutdatedFeed

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_OutdatedFeed.*feed=(?<object>[^\s]*)`	`May 2 16:41:40 alert=KL_ALERT_OutdatedFeed feed=Botnet_CnC_URL_Data_Feed.json`

- KL_ALERT_ServiceStarted

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_ServiceStarted`	`May 2 16:41:40 alert=KL_ALERT_ServiceStarted`

- KL_ALERT_ServiceStopped

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_ServiceStopped`	`May 2 16:41:40 alert=KL_ALERT_ServiceStopped`

- KL_ALERT_ServiceUnavailable

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_ServiceUnavailable`	`May 2 16:41:40 alert=KL_ALERT_ServiceUnavailable`

- KL_ALERT_UpdatedFeed

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_UpdatedFeed.*feed=(?<object>[^\s]*).*records=(?<quantity>[^\s]*)`	`May 2 16:41:40 alert=KL_ALERT_UpdatedFeed feed=Botnet_CnC_URL_Data_Feed.json records=23`

- KL_ALERT_FailedToUpdateFeed

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_FailedToUpdateFeed.*feed=(?<object>[^\s]*)`	`May 2 16:41:40 alert=KL_ALERT_FailedToUpdateFeed feed=Botnet_CnC_URL_Data_Feed.json`

- KL_ALERT_LicenseExpires

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_LicenseExpires.*license_name=(?<object>[^\s]*)`	`May 2 16:41:40 alert=KL_ALERT_LicenseExpires expiration_date=23.02.2020 license_name=kl_license`

- KL_ALERT_LicenseExpired

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_LicenseExpired.*license_name=(?<object>[^\s]*)`	`May 2 16:41:40 alert=KL_ALERT_LicenseExpired expiration_date=23.02.2020 license_name=kl_license`

- KL_ALERT_EPSLimitExceeded

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_EPSLimitExceeded.*current_eps=(?<quantity>[^\s]*)`	`May 2 16:41:40 alert=KL_ALERT_EPSLimitExceeded current_eps=6500 license_limit_eps=5000`

- KL_ALERT_EPSHardLimit

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_EPSHardLimit.*license_limit_eps=(?<quantity>[^\s]*)`	`May 2 16:41:40 alert=KL_ALERT_EPSHardLimit license_limit_eps=5000`

- KL_ALERT_LicenseChanged

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_LicenseChanged.*license_name=(?<object>[^\s]*)`	`May 2 16:41:40 alert=KL_ALERT_LicenseChanged expiration_date=23.02.2020 license_name=kl_license licensing_level=EnterpriseTIP`

- KL_ALERT_ConfigurationUpdated

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_ConfigurationUpdated`	`May 2 16:41:40 alert=KL_ALERT_ConfigurationUpdated`

- KL_ALERT_RetroScanError

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_RetroScanError.*error=(?<object>[^\s]*)`	`May 2 16:41:40 alert=KL_ALERT_RetroScanError error=Service is unavailable`

- KL_ALERT_RetroScanCompleted

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_RetroScanCompleted.*iocs_rescanned=(?<object>[^\s]*).*iocs_detected=(?<quantity>[^\s]*).*retroscan_report=(?<url>[^\s]*)`	`May 2 16:41:40 alert=KL_ALERT_RetroScanCompleted iocs_rescanned=1998 iocs_detected=82 retroscan_report=https://127.0.0.1:443/retroscan/81650945-f186-437b-8945-9f31715d32da`

- KL_ALERT_RetroScanStorageExceeded

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_RetroScanStorageExceeded.*storage_size_limit=(?<object>[^\s]*)`	`May 2 16:41:40 alert=KL_ALERT_RetroScanStorageExceeded storage_size_limit=9876`

- KL_ALERT_IndicatorsStoreHardLimit

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_IndicatorsStoreHardLimit.*license_limit_indicators=(?<quantity>[^\s]*).*msg=(?<object>[^\s]*)`	`May 2 16:41:40 alert=KL_ALERT_IndicatorsStoreHardLimit license_limit_indicators=5000000 msg=Indicators store limit exceeded`

- KL_ALERT_FreeSpaceEnds

Регулярное выражение	Пример события для проверки регулярных выражений
`alert=KL_ALERT_FreeSpaceEnds.*msg=Free space left: (?<object>[^\s]*) Mb`	`May 2 16:41:40 alert=KL_ALERT_FreeSpaceEnds msg=Free space left: 7322 Mb`

- KL_APT_Hash_MD5

Регулярное выражение	Пример события для проверки регулярных выражений
`category=KL_APT_Hash_MD5.*matchedIndicator=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=KL_APT_Hash_MD5 matchedIndicator=7A2E65A0F70EE0615EC0CA34240CF082 url=- src=192.168.0.0 ip=- md5=7A2E65A0F70EE0615EC0CA34240CF082 sha1=- sha256=- usrName=VerifTestUserName MD5=7A2E65A0F70EE0615EC0CA34240CF082 detection_date=01.06.2018 00:00 publication_name=TestRecordMb`

- KL_APT_Hash_SHA1

Регулярное выражение	Пример события для проверки регулярных выражений
`category=KL_APT_Hash_SHA1.*sha1=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=KL_APT_Hash_SHA1 matchedIndicator=7A2EE06E65A0F70EE0615EC0CA342470EE0CF082 url=- src=192.168.0.0 ip=- md5=- sha1=7A2EE06E65A0F70EE0615EC0CA342470EE0CF082 sha256=- usrName=VerifTestUserName MD5=7A2E65A0F70EE0615EC0CA34240CF082 SHA1=EA2EE06E65A0F70EE0615EC0CA342470EE0CF082 SHA256=2EE072EEA2EE615EC006E65A0CF0F70EA342E0615EC0F70ECA342470EE0CF082 detection_date=01.06.2018 00:00 publication_name=TestRecord`

- KL_APT_Hash_SHA256

Регулярное выражение	Пример события для проверки регулярных выражений
`category=KL_APT_Hash_SHA256.*sha256=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=KL_APT_Hash_SHA256 matchedIndicator=2EE072EEA2EE615EC006E65A0CF0F70EA342E0615EC0F70ECA342470E url=- src=192.168.0.0 ip=- md5=- sha1=- sha256=2EE072EEA2EE615EC006E65A0CF0F70EA342E0615EC0F70ECA342470EE0CF082 usrName=VerifTestUserName MD5=7A2E65A0F70EE0615EC0CA34240CF082 SHA1=EA2EE06E65A0F70EE0615EC0CA342470EE0CF082 SHA256=2EE072EEA2EE615EC006E65A0CF0F70EA342E0615EC0F70ECA342470EE0CF082 detection_date=01.06.2018 00:00 publication_name=TestRecord`

- KL_APT_IP

Регулярное выражение	Пример события для проверки регулярных выражений
`category=KL_APT_IP.*matchedIndicator=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=KL_APT_IP matchedIndicator=192.0.2.4 url=- src=192.168.0.0 ip=192.0.2.4 md5=- sha1=- sha256=- usrName=VerifTestUserName detection_date=01.06.2018 00:00 ip=192.0.2.4 publication_name=TestRecord`

- KL_APT_URL

Регулярное выражение	Пример события для проверки регулярных выражений
`category=KL_APT_URL.*matchedIndicator=(?<url>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=KL_APT_URL matchedIndicator=b046f5b25458638f6705d53539c79f62.com url=b046f5b25458638f6705d53539c79f62.com src=192.168.0.0 ip=- md5=- sha1=- sha256=- usrName=VerifTestUserName detection_date=01.06.2018 00:00 id=0 mask=b046f5b25458638f6705d53539c79f62.com publication_name=TestRecord type=1`

- KL_BotnetCnC_Hash_MD5

Регулярное выражение	Пример события для проверки регулярных выражений
`category=KL_BotnetCnC_Hash_MD5.*md5=(?<object>[^\s]*).*usrName=(?<login>[^\s]*).*mask=(?<url>[^\s]*).*threat=(?<objectname>[^\s]*)`	`May 2 16:41:40 category=KL_BotnetCnC_Hash_MD5 url=- md5=E013C01AB3E27BE6FBA4E23EE88B100F sha1=- sha256=- ip=- usrName=VerifTestUserName IP=118.142.224.213, 160.16.120.71, 61.19.201.7 files=[{MD5=E013C01AB3E27BE6FBA4E23EE88B100F SHA256=C00269AA2BCF375D0CF870C36F737C27EBB04F69F5B6912F860D8A1F5F1D9DF6}] first_seen=08.07.2015 23:39 geo=jp, hk, tw, au, th, cn, my, ph, vn, in id=9189405 last_seen=29.10.2015 15:59 mask=172.117.45.14/pid=1000/botnet_setup_3.exe popularity=5 threat=Trojan-Banker.AndroidOS.Wroba type=3`

- KL_BotnetCnC_Hash_SHA1

Регулярное выражение	Пример события для проверки регулярных выражений
`category=KL_BotnetCnC_Hash_SHA1.*sha1=(?<object>[^\s]*).*usrName=(?<login>[^\s]*).*mask=(?<url>[^\s]*).*threat=(?<objectname>[^\s]*)`	`May 2 16:41:40 category=KL_BotnetCnC_Hash_SHA1 url=- md5=- sha1=FE61DED0504013D9ED6691F6C5BB69DCD8C8DD60 sha256=- ip=- usrName=VerifTestUserName IP=78.47.151.188 files=[{SHA1=FE61DED0504013D9ED6691F6C5BB69DCD8C8DD60 SHA256=B6AEF9CBFA21B0A9E6D03364F5476B81C4A5D8EF212DFB35E3EF96003CADCB0B} first_seen=21.07.2015 12:19 geo=it, es, de, fr, gb id=9320249 last_seen=14.01.2016 12:55 mask=botnet_domain_4.com/get.php?p=4&id=2 popularity=4 threat=Trojan-SMS.AndroidOS.Opfake type=4`

- KL_BotnetCnC_Hash_SHA256

Регулярное выражение	Пример события для проверки регулярных выражений
`category=KL_BotnetCnC_Hash_SHA256.*sha256=(?<object>[^\s]*).*usrName=(?<login>[^\s]*).*mask=(?<url>[^\s]*).*threat=(?<objectname>[^\s]*)`	`May 2 16:41:40 category=KL_BotnetCnC_Hash_SHA256 url=- md5=- sha1=- sha256=AFDD5508B48B8270C1DBAF32121A00951E450A56791275D8E7C413EF8380A ip=- usrName=VerifTestUserName IP=46.4.114.61, 95.213.186.51, 95.213.192.71, 176.9.82.215, 178.63.12.207, 109.206.186.164, 176.9.4 213.163.70.170, 95.213.192.83, 173.45.161.113 files=[{MD5=55B8D137C80AE5E995EC355524594F3B SHA1=BEA6B860C719F1C886461C8A3FF4935471D2FA64 SHA256=AFDD5508B48B8270C1DBAF32121A00951E450A56791275D8E7C413EF8380A first_seen=15.04.2015 13:18 geo=vn, in, tr, mx, ir, bd, id, dz, ph, id=9230458 last_seen=14.01.2016 12:55 mask=*.subbotnet_domain_19.botnet_domain.com popularity=5 threat=Trojan.Win32.Agent type=19`

- KL_BotnetCnC_URL

Регулярное выражение	Пример события для проверки регулярных выражений
`category=KL_BotnetCnC_URL.*url=(?<url>[^\s]*).*usrName=(?<login>[^\s]*)`	`May 2 16:41:40 category=KL_BotnetCnC_URL url=http://d.subphishing_domain.phishing_domain_19.com md5=- sha1=- sha256=- ip=- usrName=VerifTestUserName IP=104.168.159.146, 138.201.0.229, 138.201.0.231, 138.201.0.230, 78.46.185.21, 78.46.185.23, 78.46.185.12, 78.46.185.3, 78.46.185.16, 78.46.185.28 first_seen=12.01.2016 12:50 geo=br, pt, us id=9508721 last_seen=14.01.2016 13:36 mask=*.subphishing_domain.phishing_domain_19.com popularity=5 type=19`

- KL_ICS_Hash_MD5

Регулярное выражение	Пример события для проверки регулярных выражений
`category=KL_ICS_Hash_MD5.*md5=(?<object>[^\s]*).*usrName=(?<login>[^\s]*).*threat=(?<objectname>[^\s]*)`	`May 2 16:41:40 category=KL_ICS_Hash_MD5 matchedIndicator=7A8F30B40C6564EFF95E678F7C43346C url=- src=- ip=- md5=7A8F30B40C6564EFF95E678F7C43346C sha1=- sha256=- usrName=VerifTestUserName MD5=7A8F30B40C6564EFF95E678F7C43346C SHA1=E51B1A1FDA2CAF10623A83A1476585AC6E10D569 SHA256=EF6CDD46DB5513F7247789E559A1520F6C1DCD17235C395EDCA3E5043988B54B file_size=1989 first_seen=10.07.2015 23:53 last_seen=12.10.2019 18:44 popularity=1 threat=HEUR:Trojan.Win32.Generic`

- KL_ICS_Hash_SHA1

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_ICS_Hash_SHA1.*sha1=(?<object>[^\s]*).*usrName=(?<login>[^\s]*).*threat=(?<objectname>[^\s]*)	May 2 16:41:40 category=KL_ICS_Hash_SHA1 matchedIndicator=E51B1A1FDA2CAF10623A83A1476585AC6E10D569 url=- src=- ip=- md5=- sha1=E51B1A1FDA2CAF10623A83A1476585AC6E10D569 sha256=- usrName=VerifTestUserName MD5=7A8F30B40C6564EFF95E678F7C43346C SHA1=E51B1A1FDA2CAF10623A83A1476585AC6E10D569 SHA256=EF6CDD46DB5513F7247789E559A1520F6C1DCD17235C395EDCA3E5043988B54B file_size=1989 first_seen=10.07.2015 23:53 last_seen=12.10.2019 18:44 popularity=1 threat=HEUR:Trojan.Win32.Generic

- KL_ICS_Hash_SHA256

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_ICS_Hash_SHA256.*sha256=(?<object>[^\s]*).*usrName=(?<login>[^\s]*).*threat=(?<objectname>[^\s]*)	May 2 16:41:40 category=KL_ICS_Hash_SHA256 matchedIndicator=EF6CDD46DB5513F7247789E559A1520F6C1DCD17235C395EDCA3E5043 url=- src=- ip=- md5=- sha1=- sha256=EF6CDD46DB5513F7247789E559A1520F6C1DCD17235C395EDCA3E5043988B54B usrName=VerifTestUserName MD5=7A8F30B40C6564EFF95E678F7C43346C SHA1=E51B1A1FDA2CAF10623A83A1476585AC6E10D569 SHA256=EF6CDD46DB5513F7247789E559A1520F6C1DCD17235C395EDCA3E5043988B54B file_size=1989 first_seen=10.07.2015 23:53 last_seen=12.10.2019 18:44 popularity=1 threat=HEUR:Trojan.Win32.Generic

- KL_InternalTI_URL

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_InternalTI_URL.*url=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_InternalTI_URL matchedIndicator=fakess123.nu url=fakess123.nu src=- ip=- md5=- sha1=- sha256=- usrName=VerifTestUser URL=fakess123.nu

- KL_InternalTI_IP

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_InternalTI_IP.*ip=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_InternalTI_IP matchedIndicator=192.0.2.0 url=- src=- ip=192.0.2.0 md5=- sha1=- sha256=- usrName=VerifTestUser IP=192.0.2.0

- KL_InternalTI_Hash_MD5

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_InternalTI_MD5.*md5=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_InternalTI_MD5 matchedIndicator=44D88612FEA8A8F36DE82E1278ABB02F url=- src=- ip=- md5=44D88612FEA8A8F36DE82E1278ABB02F sha1=- sha256=- usrName=VerifTestUser MD5=44D88612FEA8A8F36DE82E1278ABB02F

- KL_InternalTI_Hash_SHA1

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_InternalTI_SHA1.*sha1=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_InternalTI_SHA1 matchedIndicator=3395856CE81F2B7382DEE72602F798B642F14140 url=- src=- ip=- md5=- sha1=3395856CE81F2B7382DEE72602F798B642F14140 sha256=- usrName=VerifTestUser SHA1=3395856CE81F2B7382DEE72602F798B642F14140

- KL_InternalTI_Hash_SHA256

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_InternalTI_SHA256.*sha256=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_InternalTI_SHA256 matchedIndicator=762B2BE1D22B737A287D0D6D4FBAF983FD214BBA1497C0A3A2C58C7 url=- src=- ip=- md5=- sha1=- sha256=762B2BE1D22B737A287D0D6D4FBAF983FD214BBA1497C0A3A2C58C7819303C0C usrName=VerifTestUser SHA256=762B2BE1D22B737A287D0D6D4FBAF983FD214BBA1497C0A3A2C58C7819303C0C

- KL_IP_Reputation

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_IP_Reputation\s.*ip=(?<object>[^\s]*).*usrName=(?<login>[^\s]*).*category=(?<process>[^\s]*).*threat_score=(?<severity>[^\s]*)	May 2 16:41:40 category=KL_IP_Reputation url=- md5=- sha1=- sha256=- ip=18.50.1.47 usrName=VerifiTestUserName category=spam first_seen=21.01.2015 00:00 ip=18.50.1.47 ip_geo=us last_seen=17.05.2016 03:16 popularity=1 threat_score=100

- KL_IP_Reputation_Hash_MD5

Регулярное выражение	Пример события для проверки регулярных выражени
category=KL_IP_Reputation_Hash_MD5.*matchedIndicator=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_IP_Reputation_Hash_MD5 matchedIndicator=61200D253ADD14C91CD64F2CB1F221CB url=- s md5=61200D253ADD14C91CD64F2CB1F221CB sha1=- sha256=- usrN category=malware domains=k4d7ppv9.humanpchelp.pw, mwi49i2b.backbonecomputer.top, 9uq5mmw7.overseascomputer. 9tqnii2s.motivationcomputer.pw, 4iaag9ng.luxurypchelp.pw, kxol25kx.pcserviceline.top, 7ifiye96.phoenixcomputerhelp. tnv5yyvj.pcservicecatch.pw, y4ki19os.computercoral.top, pmayaidy.rankpcservice.top files=[{ MD5=61200D253ADD14C91CD64F2CB1F221CB SHA1=E23B0F6ECEFF56870908B2EC704F62ACB4E005AD SHA256=7FC582451A8D9EAF112A3CFC7EFF8EBC8A5FCB8480E42A8D2B threat=HEUR:Trojan.Script.Generic},{ MD5=06A2E41E9CDA9C19AF5FB29483687A56 SHA1=37ED2076FCC0365BA02210E18BBAB162D7338180 SHA256=9570F5C81FF906CD52EE42B5D24359B8A7CA4EC225C532A811 threat=HEUR:Trojan.Script.Generic},{ MD5=AA909F4A33A0D305C0ADF7FCD6DC95E5 SHA1=0A88A71A3C43F02075B7B3CB1A6ED1A603CC666E SHA256=96467635B09D64B29DEAF2A7923ADCD63C2E7F9308B80DDF46 threat=HEUR:Trojan.Script.Generic},{ MD5=1D02D52FE17A040A2C7D7C4EE7020E6A SHA1=036D8147D00334824073A22C3D7016EE27643CBD SHA256=737117D867D8CC777AF09F635126C6867ADD08C47C74EDCF56 threat=HEUR:Trojan.Script.Generic},{ MD5=393F797A732D5FF35B6102B298349C65 SHA1=760C99F3FB4330BA7B9EB76780718E3023C345EE SHA256=5E86FE0A4DA6A1394DBC6BD2D0F7BD2791BCC1099F83B04282 threat=HEUR:Trojan.Script.Generic},{ MD5=5A90DDAAEA8646E84927E5DD7BAAA3E2 SHA1=CA2EEF839CF649E42EB4F7E618BD491B40340462 SHA256=1A73D4EA89E89C22B3B03E1A841882A59FCC1ED18299D6914D threat=HEUR:Trojan.Script.Generic}] first_seen=21.02.2019 ip=93.115.27.83 ip_geo=lt ip_whois={ asn=16125 country=LT created=01.12.2016 net_name=CHERRYSERVERS-LT-DEDICATED net_range=93.115.27.0 - 93.115.27.255 updated=01.12.2016} last_seen=22.05.2019 19:18 popularity=5 threat_score=94 u jp, fr, it, ch, at, be, pl, es, dz

- KL_IP_Reputation_Hash_SHA1

Регулярное выражение	Пример события для проверки регулярных выражен
category=KL_IP_Reputation_Hash_SHA1.*matchedIndicator=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_IP_Reputation_Hash_SHA1 matchedIndicator=E23B0F6ECEFF56870908B2EC704F62ACB4E005A ip=- md5=- sha1=E23B0F6ECEFF56870908B2EC704F62ACB4E005AD usrName=- category=malware domains=k4d7ppv9.humanpchelp. mwi49i2b.backbonecomputer.top, 9uq5mmw7.overseascomputer 9tqnii2s.motivationcomputer.pw, 4iaag9ng.luxurypchelp.pw kxol25kx.pcserviceline.top, 7ifiye96.phoenixcomputerhelp tnv5yyvj.pcservicecatch.pw, y4ki19os.computercoral.top, pmayaidy.rankpcservice.top files=[{ MD5=61200D253ADD14C91CD64F2CB1F221CB SHA1=E23B0F6ECEFF56870908B2EC704F62ACB4E005AD SHA256=7FC582451A8D9EAF112A3CFC7EFF8EBC8A5FCB8480E42A8D2 threat=HEUR:Trojan.Script.Generic},{ MD5=06A2E41E9CDA9C19AF5FB29483687A56 SHA1=37ED2076FCC0365BA02210E18BBAB162D7338180 SHA256=9570F5C81FF906CD52EE42B5D24359B8A7CA4EC225C532A81 threat=HEUR:Trojan.Script.Generic},{ MD5=AA909F4A33A0D305C0ADF7FCD6DC95E5 SHA1=0A88A71A3C43F02075B7B3CB1A6ED1A603CC666E SHA256=96467635B09D64B29DEAF2A7923ADCD63C2E7F9308B80DDF4 threat=HEUR:Trojan.Script.Generic},{ MD5=1D02D52FE17A040A2C7D7C4EE7020E6A SHA1=036D8147D00334824073A22C3D7016EE27643CBD SHA256=737117D867D8CC777AF09F635126C6867ADD08C47C74EDCF5 threat=HEUR:Trojan.Script.Generic},{ MD5=393F797A732D5FF35B6102B298349C65 SHA1=760C99F3FB4330BA7B9EB76780718E3023C345EE SHA256=5E86FE0A4DA6A1394DBC6BD2D0F7BD2791BCC1099F83B0428 threat=HEUR:Trojan.Script.Generic},{ MD5=5A90DDAAEA8646E84927E5DD7BAAA3E2 SHA1=CA2EEF839CF649E42EB4F7E618BD491B40340462 SHA256=1A73D4EA89E89C22B3B03E1A841882A59FCC1ED18299D6914 threat=HEUR:Trojan.Script.Generic}] first_seen=21.02.201 ip=93.115.27.83 ip_geo=lt ip_whois={ asn=16125 country=L created=01.12.2016 net_name=CHERRYSERVERS-LT-DEDICATED net_range=93.115.27.0 - 93.115.27.255 updated=01.12.2016 last_seen=22.05.2019 19:18 popularity=5 threat_score=94 jp, fr, it, ch, at, be, pl, es, dz

- KL_IP_Reputation_Hash_SHA256

Регулярное выражение	Пример события для проверки регулярных
category=KL_IP_Reputation_Hash_SHA256.*matchedIndicator=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_IP_Reputation_Hash_SHA256 matchedIndicator=7FC582451A8D9EAF112A3CFC7EFF8EBC8A5FC url=- src=- ip=- md5=- sha1=- sha256=7FC582451A8D9EAF112A3CFC7EFF8EBC8A5FCB8480E42A8 category=malware domains=k4d7ppv9.humanpchelp.pw, mwi4 9uq5mmw7.overseascomputer.pw, 9tqnii2s.motivationcompu 4iaag9ng.luxurypchelp.pw, kxol25kx.pcserviceline.top, 7ifiye96.phoenixcomputerhelp.pw, tnv5yyvj.pcservicecat y4ki19os.computercoral.top, pmayaidy.rankpcservice.top MD5=61200D253ADD14C91CD64F2CB1F221CB SHA1=E23B0F6ECEFF56870908B2EC704F62ACB4E005AD SHA256=7FC582451A8D9EAF112A3CFC7EFF8EBC8A5FCB8480E42A8 threat=HEUR:Trojan.Script.Generic},{ MD5=06A2E41E9CDA9 SHA1=37ED2076FCC0365BA02210E18BBAB162D7338180 SHA256=9570F5C81FF906CD52EE42B5D24359B8A7CA4EC225C532A threat=HEUR:Trojan.Script.Generic},{ MD5=AA909F4A33A0D SHA1=0A88A71A3C43F02075B7B3CB1A6ED1A603CC666E SHA256=96467635B09D64B29DEAF2A7923ADCD63C2E7F9308B80DD threat=HEUR:Trojan.Script.Generic},{ MD5=1D02D52FE17A0 SHA1=036D8147D00334824073A22C3D7016EE27643CBD SHA256=737117D867D8CC777AF09F635126C6867ADD08C47C74EDC threat=HEUR:Trojan.Script.Generic},{ MD5=393F797A732D5 SHA1=760C99F3FB4330BA7B9EB76780718E3023C345EE SHA256=5E86FE0A4DA6A1394DBC6BD2D0F7BD2791BCC1099F83B04 threat=HEUR:Trojan.Script.Generic},{ MD5=5A90DDAAEA864 SHA1=CA2EEF839CF649E42EB4F7E618BD491B40340462 SHA256=1A73D4EA89E89C22B3B03E1A841882A59FCC1ED18299D69 threat=HEUR:Trojan.Script.Generic}] first_seen=21.02.2 ip_geo=lt ip_whois={ asn=16125 country=LT created=01.1 net_name=CHERRYSERVERS-LT-DEDICATED net_range=93.115.2 updated=01.12.2016} last_seen=22.05.2019 19:18 popular users_geo=de, jp, fr, it, ch, at, be, pl, es, dz

- KL_Malicious_Hash_MD5

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_Malicious_Hash_MD5.*md5=(?<object>[^\s]*).*usrName=(?<login>[^\s]*).*file_size=(?<size>[^\s]*).*threat=(?<objectname>[^\s]*)	May 2 16:41:40 category=KL_Malicious_Hash_MD5 url=- md5=0F1DCBB2A888B99FAE72144087CAE565 sha1=- sha256=- ip=- usrName=VerifTestUserName MD5=0F1DCBB2A888B99FAE72144087CAE565 file_size=105472 file_type=PE first_seen=26.11.2015 13:06 geo=ru, ro, ua, tj, us, cz, kz, gb last_seen=14.01.2016 12:29 popularity=5 threat=UDS:DangerousObject.Multi.Generic

- KL_Malicious_Hash_SHA1

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_Malicious_Hash_SHA1.*sha1=(?<object>[^\s]*).*usrName=(?<login>[^\s]*).*file_size=(?<size>[^\s]*).*threat=(?<objectname>[^\s]*)	May 2 16:41:40 category=KL_Malicious_Hash_SHA1 url=- md5=- sha1=6665856CE81F2B7382DEE72602F798B642F14140 sha256=- ip=- usrName=VerifTestUserName MD5=55D88612FEA8A8F36DE82E1278ABB02F SHA1=6665856CE81F2B7382DEE72602F798B642F14140 SHA256=275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4777AABF651FD0F file_size=68 first_seen=02.04.2010 22:07 last_seen=14.01.2016 13:41 popularity=5 threat=EICAR-Test-File

- KL_Malicious_Hash_SHA256

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_Malicious_Hash_SHA256.*sha256=(?<object>[^\s]*).*usrName=(?<login>[^\s]*).*file_size=(?<size>[^\s]*).*threat=(?<objectname>[^\s]*)	May 2 16:41:40 category=KL_Malicious_Hash_SHA256 url=- md5=- sha1=- sha256=EC1D5E24A9F866F21118914445AB0A00A60F791B51478F3D0DD375A6BD458 ip=- usrName=VerifTestUserName SHA1=C365DC5128FF0A607D78BFBAB36E08263DC66B18 SHA256=EC1D5E24A9F866F21118914445AB0A00A60F791B51478F3D0DD375A6BD458 file_size=1696256 file_type=PE first_seen=15.07.2015 11:50 geo=ru, u by, dz, ir, eg, kz, mx, in, tr last_seen=14.01.2016 12:29 popularity threat=HackTool.Win32.KRT.bw

- KL_Malicious_URL

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_Malicious_URL\s.*url=(?<url>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_Malicious_URL url=http://sub1.submalicious_domain.malicious_domain_19.com md5=- sha1=- sha256=- ip=- usrName=VerifTestUserName IP=217.23.14.223 first_seen=14.01.2016 02:42 geo=ru, kz, ro, ua, by, cz id=9524476 last_seen=14.01.2016 13:36 mask=*.submalicious_domain.malicious_domain_19.com popularity=5 type=19

- KL_Malicious_URL_Hash_MD5

Регулярное выражение	Пример события для проверки регулярных выражени
category=KL_Malicious_URL_Hash_MD5.*matchedIndicator=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_Malicious_URL_Hash_MD5 matchedIndicator=C735608E2DDE63857C3877AE438EBF78 url=- s md5=C735608E2DDE63857C3877AE438EBF78 sha1=- sha256=- usrN IP=104.27.160.251, 104.27.161.251, 145.239.252.74, 46.35. 207.244.89.108, 54.37.87.37, 207.244.89.90, 77.111.246.8, category=Malware files=[{ MD5=C735608E2DDE63857C3877AE438 SHA1=9FB04AB8756742E9903A9A77566938DC9D83138C SHA256=127E83998D65FD80328D89B87B9C4CB5756C57FCC03189FAC5 threat=HEUR:Trojan.Script.Miner.gen}] first_seen=15.03.20 geo=es, de, it, ru, ve, pl, pt, jp, kz, mx id=29703667 last_seen=23.05.2019 14:12 mask=tercabilis.info popularit whois={ NS=art.ns.cloudflare.com, olga.ns.cloudflare.com NS_ips=173.245.58.137, 173.245.59.102 country=FR created= domain=tercabilis.info expires=02.10.2019 org=NETIM registrar_name=NETIM SARL updated=01.12.2018}

- KL_Malicious_URL_Hash_SHA1

Регулярное выражение	Пример события для проверки регулярных выражен
category=KL_Malicious_URL_Hash_SHA1.*matchedIndicator=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_Malicious_URL_Hash_SHA1 matchedIndicator=9FB04AB8756742E9903A9A77566938DC9D83138 ip=- md5=- sha1=9FB04AB8756742E9903A9A77566938DC9D83138C usrName=- IP=163.172.129.78, 212.47.250.90 category=Malw MD5=9096549542B5A4E711BF04732416AA97 SHA1=4616FF9FBFF692535C6F0D9BD347CC0593A1F6B8 threat=HEUR:Trojan.Script.Miner.gen},{ MD5=6CBF2B0ADC72F64913EDE949A3F93B2D SHA1=5BB602A5A3AE5C685F0EB9CF2BFE9546DFC5832A SHA256=E804F6ADF2B7C99A8E0B158E880DF3172131CFAD7D796A75C threat=HEUR:Trojan.Script.Miner.gen},{ MD5=C735608E2DDE63857C3877AE438EBF78 SHA1=9FB04AB8756742E9903A9A77566938DC9D83138C SHA256=127E83998D65FD80328D89B87B9C4CB5756C57FCC03189FAC threat=HEUR:Trojan.Script.Miner.gen}] first_seen=29.05.2 geo=ru, kz, by, ua id=23128232 last_seen=23.03.2019 12:0 mask=play.on.animeteatr.ru popularity=3 type=2

- KL_Malicious_URL_Hash_SHA256

Регулярное выражение	Пример события для проверки регулярных
category=KL_Malicious_URL_Hash_SHA256.*matchedIndicator=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_Malicious_URL_Hash_SHA256 matchedIndicator=127E83998D65FD80328D89B87B9C4CB5756C5 url=- src=- ip=- md5=- sha1=- sha256=127E83998D65FD80328D89B87B9C4CB5756C57FCC03189F IP=163.172.129.78, 212.47.250.90, 173.192.191.169, 167 category=Malware files=[{ MD5=C735608E2DDE63857C3877AE SHA1=9FB04AB8756742E9903A9A77566938DC9D83138C SHA256=127E83998D65FD80328D89B87B9C4CB5756C57FCC03189F threat=HEUR:Trojan.Script.Miner.gen},{ MD5=978E8C1CB07 SHA1=AFAEEE65BB483994FAC36A6B97F10B2BAA51F832 SHA256=3CFAACB2E8EE3E7CC5685DEDDFED7E34BF7595015307FEE threat=HEUR:Trojan.Script.Miner.gen},{ MD5=9096549542B SHA1=4616FF9FBFF692535C6F0D9BD347CC0593A1F6B8 threat=HEUR:Trojan.Script.Miner.gen},{ MD5=3FF0CF473B1 SHA1=6813E9BB538F4AE1290411DD6AC48D615B5A4F21 threat=HEUR:Trojan.Script.Miner.gen},{ MD5=6CBF2B0ADC7 SHA1=5BB602A5A3AE5C685F0EB9CF2BFE9546DFC5832A SHA256=E804F6ADF2B7C99A8E0B158E880DF3172131CFAD7D796A7 threat=HEUR:Trojan.Script.Miner.gen},{ MD5=44A27780FD4 SHA1=C9552F0DBF8A213556F3CC0CBD98CBFD157362F9 SHA256=EB703A25657D70CD85059A1AFD4720DF5273C4775EE05C6 threat=HEUR:Trojan.Script.Miner.gen}] first_seen=29.05 gb, pl, dz, hu, at, br, ch id=23128262 last_seen=07.04 mask=play.play1.videos.vidto.me popularity=4 type=2 wh mail2.vidto.me MX_ips=158.69.116.96 NS=pns1.cloudns.ne pns3.cloudns.net, pns4.cloudns.net NS_ips=185.136.96.1 185.136.98.111, 185.136.99.111 country=SE created=21.0 expires=21.06.2021 org=Shield Whois registrar_name=AB

- KL_Mobile_BotnetCnC_Hash_MD5

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_Mobile_BotnetCnC_Hash_MD5.*url=(?<url>[^\s]*).*usrName=(?<login>[^\s]*).*Mask=(?<object>[^\s{}]*)	May 2 16:41:40 category=KL_Mobile_BotnetCnC_Hash_MD5 url=- md5=12B8D137C80AE5E995EC355524594F3B sha1=- sha256=- ip=- usrName=VerifTestUserName Behaviour=Get Location, Collect phone info, Read SMS, Get Accounts, Read Contacts Details=[{Mask=*.subdbotnet_domain_19.dbotnet_domain.com}] MD5=12B8D137C80AE5E995EC355524594F3B

- KL_Mobile_BotnetCnC_Hash_SHA1

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_Mobile_BotnetCnC_Hash_SHA1.*sha1=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_Mobile_BotnetCnC_Hash_SHA1 url=- md5=- sha1=AFAEEE65BB483994FAC36A6B97F10B2BAA51F832 sha256=- ip=- usrName=VerifTestUserName Behaviour=Get Location, Collect phone info, Read SMS, Get Accounts, Read Contacts

- KL_Mobile_BotnetCnC_Hash_SHA256

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_Mobile_BotnetCnC_Hash_SHA256.*sha256=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_Mobile_BotnetCnC_Hash_SHA256 url=- sha1=- sha256=E804F6ADF2B7C99A8E0B158E880DF3172131CFAD7D796A75CBC2E4 ip=- usrName=VerifTestUserName Behaviour=Get Location, Collec info, Read SMS, Get Accounts, Read Contacts

- KL_Mobile_BotnetCnC_URL

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_Mobile_BotnetCnC_URL.*url=(?<url>[^\s]*).*usrName=(?<login>[^\s]*).*Mask=(?<object>[^\s{}]*)	May 2 16:41:40 category=KL_Mobile_BotnetCnC_URL url=baddomain.subdbotnet_domain_19.dbotnet_domain.com md5=- sha1=- sha256=- ip=- usrName=VerifTestUserName Behaviour=Get Location, Collect phone info, Read SMS, Get Accounts, Read Contacts Details=[{Mask=*.subdbotnet_domain_19.dbotnet_domain.com}] MD5=12B8D137C80AE5E995EC355524594F3B

- KL_Mobile_Malicious_Hash_MD5

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_Mobile_Malicious_Hash_MD5.*md5=(?<object>[^\s]*).*usrName=(?<login>[^\s]*).*file_size=(?<size>[^\s]*).*threat=(?<objectname>[^\s]*)	May 2 16:41:40 category=KL_Mobile_Malicious_Hash_MD5 url=- md5=A0D02A618E0FB400EDC0E210DD975E21 sha1=- sha256=- ip=- usrName=VerifTestUserName MD5=A0D02A618E0FB400EDC0E210DD975E21 SHA1=AB04F1F9CFE33EADB7ECC75EDF7A79EE1E22AEE6 SHA256=5E658421AE871ED9EA85A352050B7F27525821649EA0A6863B62BA7BDED2 file_size=378980 first_seen=10.09.2015 06:47 geo=ru, in, id, ir, my bd, ua, br, dz, ro last_seen=14.01.2016 13:18 popularity=5 threat=HEUR:Trojan.AndroidOS.Guerrilla.b

- KL_Mobile_Malicious_Hash_SHA1

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_Mobile_Malicious_Hash_SHA1.*sha1=(?<object>[^\s]*).*usrName=(?<login>[^\s]*).*file_size=(?<size>[^\s]*).*threat=(?<objectname>[^\s]*)	May 2 16:41:40 category=KL_Mobile_Malicious_Hash_SHA1 url=- md5=- sha1=9DA11F40D00E37D27A7B41EE7C741F4CF0E52AE6 sha256=- ip=- usrName=VerifTestUserName MD5=F9E8AB7B3E0B23203B678772AFD4CDD1 SHA1=9DA11F40D00E37D27A7B41EE7C741F4CF0E52AE6 SHA256=111319613DA28D6D59282EBC2730E0448717CD55B36050B91421679360 file_size=236096 first_seen=15.12.2015 20:59 geo=ru, ua, in, tr, dz, mx, kz, by, ro last_seen=14.01.2016 13:23 popularity=5 threat=HEUR:Trojan.AndroidOS.Ztorg.a

- KL_Mobile_Malicious_Hash_SHA256

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_Mobile_Malicious_Hash_SHA256.*sha256=(?<object>[^\s]*).*usrName=(?<login>[^\s]*).*file_size=(?<size>[^\s]*).*threat=(?<objectname>[^\s]*)	May 2 16:41:40 category=KL_Mobile_Malicious_Hash_SHA256 url=- sha1=- sha256=3F52BBBA93A3C757D781ED4D8D526632995FD2F712788D24C528B2 ip=- usrName=VerifTestUserName MD5=A8315A5D4C8ACB982372C16B83 SHA1=ABBB5A760C3203CB460D60279269F5568D89F848 SHA256=3F52BBBA93A3C757D781ED4D8D526632995FD2F712788D24C528B2 file_size=444408 first_seen=01.08.2015 00:08 geo=ru, ua, kz, cn, tj, uz, az, md last_seen=14.01.2016 13:18 popularity=5 threat=HEUR:Trojan-SMS.AndroidOS.Podec.a

- KL_Phishing_URL

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_Phishing_URL.*url=(?<url>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_Phishing_URL url=http://d.subphishing_domain.phishing_domain_19.com md5=- sha1=- sha256=- ip=- usrName=VerifTestUserName IP=104.168.159.146, 138.201.0.229, 138.201.0.231, 138.201.0.230, 78.46.185.21, 78.46.185.23, 78.46.185.12, 78.46.185.3, 78.46.185.16, 78.46.185.28 first_seen=12.01.2016 12:50 geo=br, pt, us id=9508721 last_seen=14.01.2016 13:36 mask=*.subphishing_domain.phishing_domain_19.com popularity=5 type=19

- KL_Ransomware_URL

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_Ransomware_URL\s.*url=(?<url>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_Ransomware_URL matchedIndicator=fakess123r.nu url=fakess123r.nu src=192.168.0.0 ip=- md5=- sha1=- sha256=- usrName=VerifTestUserName first_seen=10.08.2016 14:18 id=0 last_seen=22.12.2017 15:12 mask=fakess123r.nu popularity=1 type=1

- KL_Ransomware_URL_Hash_MD5

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_Ransomware_URL_Hash_MD5.*md5=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_Ransomware_URL_Hash_MD5 matchedIndicator=DAFECEDABFE0F3AB372A7C83B84CEFF6 url=- src=- ip=- md5=DAFECEDABFE0F3AB372A7C83B84CEFF6 sha1=- sha256=- usrName=- IP=104.27.174.162, 104.27.175.162, 188.166.67.166, 193.176.84.67, 185.232.23.3, 5.182.27.20, 178.128.153.190, 78.24.218.108, 158.58.172.76, 2.59.214.27 files=[{ MD5=DAFECEDABFE0F3AB372A7C83B84CEFF6 SHA1=0D68EE713180A5BF73F7C74CE00F067D2BE5CF7C SHA256=7DD78D2CBFF85A80954558C5C01986FC5D9099C87ECE796A374626EB76BE03 threat=HEUR:Trojan.Win32.Generic}] first_seen=01.04.2019 18:17 geo=ru kz, ua, by, de, lt, ro, pl, md, it id=30341045 last_seen=23.05.2019 14:19 mask=sama-berli.info popularity=5 type=1 whois={ NS=dora.ns.cloudflare.com, zod.ns.cloudflare.com NS_ips=173.245.58.10 173.245.59.250 country=UA created=24.01.2019 domain=sama-berli.info expires=24.01.2020 org=ZAO Sigva registrar_email=abuse@reg.ru registrar_name=Limited Liability Company "Registrar of domain names REG.RU" updated=29.03.2019}

- KL_Ransomware_URL_Hash_SHA1

Регулярное выражение	Пример события для проверки регулярных выраже
category=KL_Ransomware_URL_Hash_SHA1.*matchedIndicator=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_Ransomware_URL_Hash_SHA1 matchedIndicator=0D68EE713180A5BF73F7C74CE00F067D2BE5CF ip=- md5=- sha1=0D68EE713180A5BF73F7C74CE00F067D2BE5CF7 usrName=- IP=104.27.174.162, 104.27.175.162, 188.166.67 193.176.84.67, 185.232.23.3, 5.182.27.20, 178.128.153.1 78.24.218.108, 158.58.172.76, 2.59.214.27 files=[{ MD5=DAFECEDABFE0F3AB372A7C83B84CEFF6 SHA1=0D68EE713180A5BF73F7C74CE00F067D2BE5CF7C SHA256=7DD78D2CBFF85A80954558C5C01986FC5D9099C87ECE796A threat=HEUR:Trojan.Win32.Generic}] first_seen=01.04.201 kz, ua, by, de, lt, ro, pl, md, it id=30341045 last_see 14:19 mask=sama-berli.info popularity=5 type=1 whois={ NS=dora.ns.cloudflare.com, zod.ns.cloudflare.com NS_ips 173.245.59.250 country=UA created=24.01.2019 domain=sam expires=24.01.2020 org=ZAO Sigva registrar_email=abuse@ registrar_name=Limited Liability Company "Registrar of REG.RU" updated=29.03.2019}

- KL_Ransomware_URL_Hash_SHA256

Регулярное выражение	Пример события для проверки регулярных
category=KL_Ransomware_URL_Hash_SHA256.*matchedIndicator=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_Ransomware_URL_Hash_SHA256 matchedIndicator=7DD78D2CBFF85A80954558C5C01986FC5D90 url=- src=- ip=- md5=- sha1=- sha256=7DD78D2CBFF85A80954558C5C01986FC5D9099C87ECE79 IP=104.27.174.162, 104.27.175.162, 188.166.67.166, 19 5.182.27.20, 178.128.153.190, 78.24.218.108, 158.58.1 MD5=DAFECEDABFE0F3AB372A7C83B84CEFF6 SHA1=0D68EE713180A5BF73F7C74CE00F067D2BE5CF7C SHA256=7DD78D2CBFF85A80954558C5C01986FC5D9099C87ECE79 threat=HEUR:Trojan.Win32.Generic}] first_seen=01.04.2 by, de, lt, ro, pl, md, it id=30341045 last_seen=23.0 berli.info popularity=5 type=1 whois={ NS=dora.ns.clo zod.ns.cloudflare.com NS_ips=173.245.58.108, 173.245. created=24.01.2019 domain=sama-berli.info expires=24. registrar_email=abuse@reg.ru registrar_name=Limited L of domain names REG.RU" updated=29.03.2019}

- KL_IoT_Hash_MD5

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_IoT_Hash_MD5.*md5=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_IoT_Hash_MD5 matchedIndicator=DAFECEDABFE0F3AB372A7C83B84CEFF6 url=- src=- ip=- md5=DAFECEDABFE0F3AB372A7C83B84CEFF6 sha1=- sha256=- usrName=- IP=104.27.174.162, 104.27.175.162, 188.166.67.166, 193.176.84.67, 185.232.23.3, 5.182.27.20, 178.128.153.190, 78.24.218.108, 158.58.172.76, 2.59.214.27 files=[{ MD5=DAFECEDABFE0F3AB372A7C83B84CEFF6 SHA1=0D68EE713180A5BF73F7C74CE00F067D2BE5CF7C SHA256=7DD78D2CBFF85A80954558C5C01986FC5D9099C87ECE796A374626EB76BE037D threat=HEUR:Trojan.Win32.Generic}] first_seen=01.04.2019 18:17 geo=ru, kz, ua, by, de, lt, ro, pl, md, it id=30341045 last_seen=23.05.2019 14:19 mask=sama-berli.info popularity=5 type=1 whois={ NS=dora.ns.cloudflare.com, zod.ns.cloudflare.com NS_ips=173.245.58.108, 173.245.59.250 country=UA created=24.01.2019 domain=sama-berli.info expires=24.01.2020 org=ZAO Sigva registrar_email=abuse@reg.ru registrar_name=Limited Liability Company "Registrar of domain names REG.RU" updated=29.03.2019}

- KL_IoT_Hash_SHA1

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_IoT_Hash_SHA1.*sha1=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_IoT_Hash_MD5 matchedIndicator=0D68EE713180A5BF73F7C74CE00F067D2BE5CF7C url=- src=- ip=- md5=- sha1=0D68EE713180A5BF73F7C74CE00F067D2BE5CF7C sha256=- usrName=- IP=104.27.174.162, 104.27.175.162, 188.166.67.166, 193.176.84.67, 185.232.23.3, 5.182.27.20, 178.128.153.190, 78.24.218.108, 158.58.172.76, 2.59.214.27 files=[{ MD5=DAFECEDABFE0F3AB372A7C83B84CEFF6 SHA1=0D68EE713180A5BF73F7C74CE00F067D2BE5CF7C SHA256=7DD78D2CBFF85A80954558C5C01986FC5D9099C87ECE796A374626EB76BE037D threat=HEUR:Trojan.Win32.Generic}] first_seen=01.04.2019 18:17 geo=ru, kz, ua, by, de, lt, ro, pl, md, it id=30341045 last_seen=23.05.2019 14:19 mask=sama-berli.info popularity=5 type=1 whois={ NS=dora.ns.cloudflare.com, zod.ns.cloudflare.com NS_ips=173.245.58.108, 173.245.59.250 country=UA created=24.01.2019 domain=sama-berli.info expires=24.01.2020 org=ZAO Sigva registrar_email=abuse@reg.ru registrar_name=Limited Liability Company "Registrar of domain names REG.RU" updated=29.03.2019}

- KL_IoT_Hash_SHA256

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_IoT_URL.*url=(?<url>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_IoT_Hash_SHA256 matchedIndicator=7DD78D2CBFF85A80954558C5C01986FC5D9099C87ECE796A374626EB76BE037D url=- src=- ip=- md5=- sha1=- sha256=7DD78D2CBFF85A80954558C5C01986FC5D9099C87ECE796A374626EB76BE037D usrName=- IP=104.27.174.162, 104.27.175.162, 188.166.67.166, 193.176.84.67, 185.232.23.3, 5.182.27.20, 178.128.153.190, 78.24.218.108, 158.58.172.76, 2.59.214.27 files=[{ MD5=DAFECEDABFE0F3AB372A7C83B84CEFF6 SHA1=0D68EE713180A5BF73F7C74CE00F067D2BE5CF7C SHA256=7DD78D2CBFF85A80954558C5C01986FC5D9099C87ECE796A374626EB76BE037D threat=HEUR:Trojan.Win32.Generic}] first_seen=01.04.2019 18:17 geo=ru, kz, ua, by, de, lt, ro, pl, md, it id=30341045 last_seen=23.05.2019 14:19 mask=sama-berli.info popularity=5 type=1 whois={ NS=dora.ns.cloudflare.com, zod.ns.cloudflare.com NS_ips=173.245.58.108, 173.245.59.250 country=UA created=24.01.2019 domain=sama-berli.info expires=24.01.2020 org=ZAO Sigva registrar_email=abuse@reg.ru registrar_name=Limited Liability Company "Registrar of domain names REG.RU" updated=29.03.2019}

- KL_IoT_URL

Регулярное выражение	Пример события для проверки регулярных выражений
category=KL_IoT_Hash_SHA256.*sha256=(?<object>[^\s]*).*usrName=(?<login>[^\s]*)	May 2 16:41:40 category=KL_IoT_URL matchedIndicator=fakess123r.nu url=fakess123r.nu src=192.168.0.0 ip=- md5=- sha1=- sha256=- usrName=VerifTestUserName first_seen=10.08.2016 14:18 id=0 last_seen=22.12.2017 15:12 mask=fakess123r.nu popularity=1 type=1

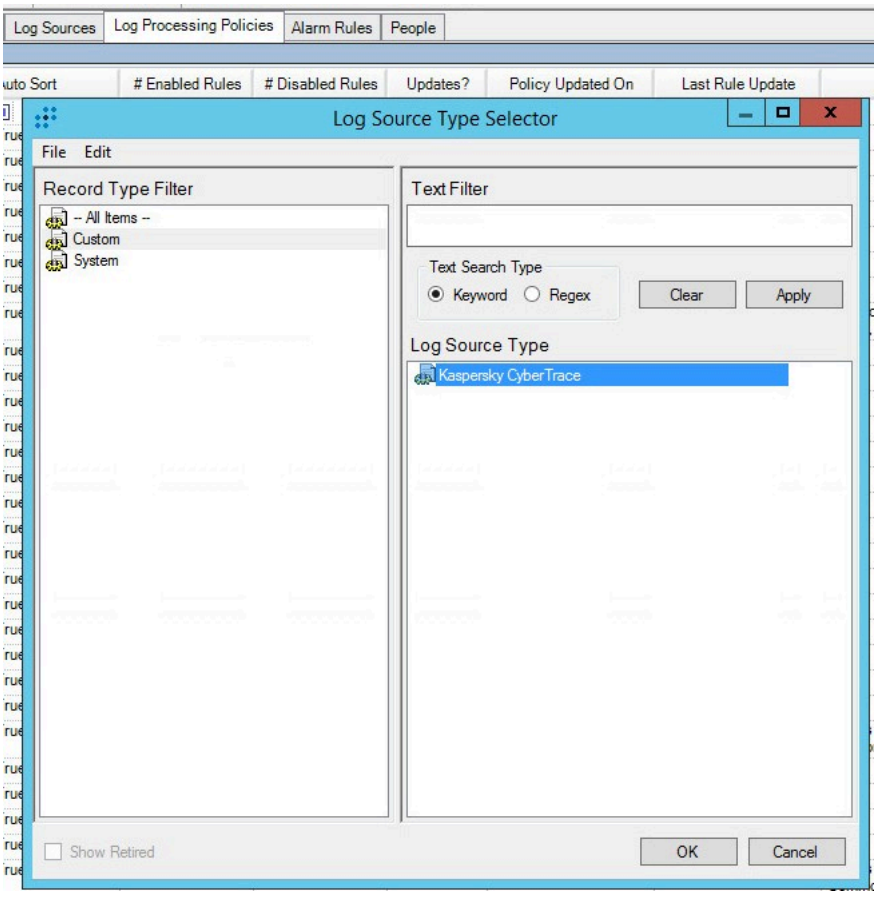
Шаг 5. Добавление политики Kaspersky CyberTrace

В этом разделе описывается порядок добавления политики Kaspersky CyberTrace в LogRhythm.

Чтобы добавить политику Kaspersky CyberTrace в LogRhythm, выполните следующие действия:

1. Запустите LogRhythm Console.
2. Выберите **Deployment Manager** → **Log Processing Policies**.
3. Нажмите на кнопку **New** ( ).

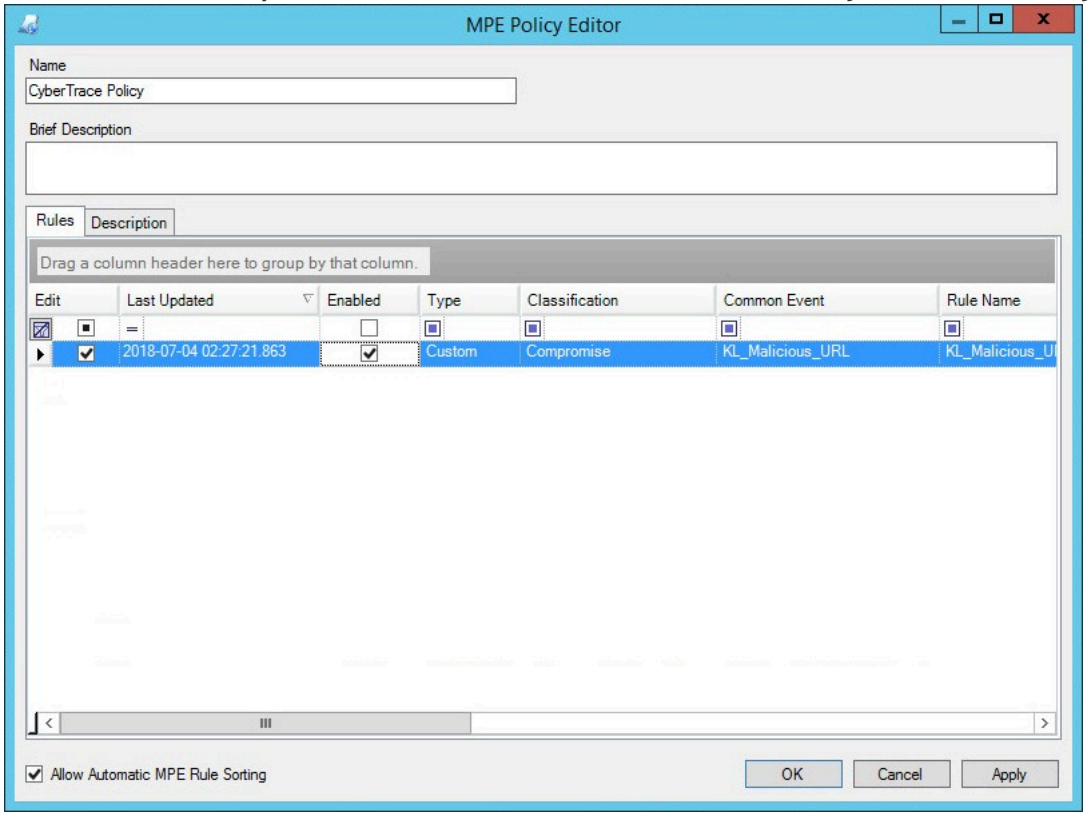
   Откроется окно **Log Source Type Selector**.



Окно **Log Source Type Selector**

4. В списке **Log Source Type** выберите **Kaspersky CyberTrace**.
5. Нажмите на кнопку **OK**.

6. В открывшемся окне **MPE Policy Editor** в поле **Name** введите имя политики (`CyberTrace Policy`).



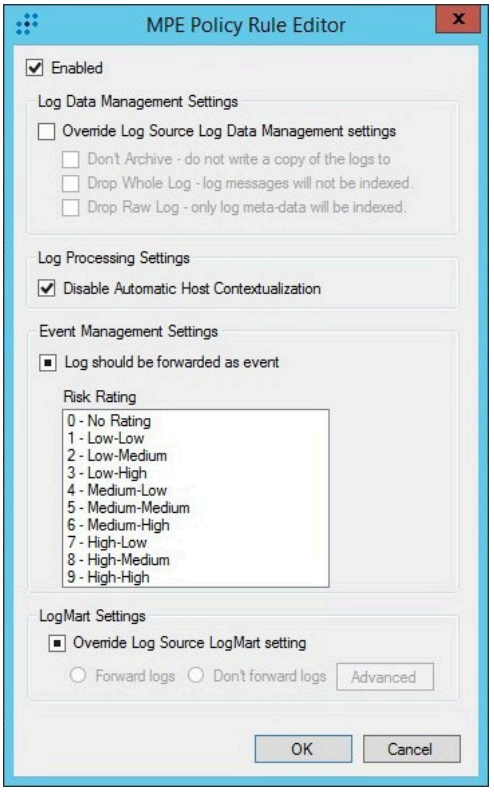
Окно **MPE Policy Editor**

7. На вкладке **Rules** измените свойства событий Kaspersky CyberTrace:

   a. Установите все флажки для каждого события.

   b. Щелкните правой кнопкой мыши в таблице и выберите **Properties**.

Откроется окно **MPE Policy Rule Editor**.



Окно **MPE Policy Rule Editor**

8. В окне **MPE Policy Rule Editor** установите флажок **Enabled**, но не меняйте состояние остальных флажков.

9. Нажмите на кнопку **OK**.

Шаг 6. Добавление источника журналов в System Monitor Agent

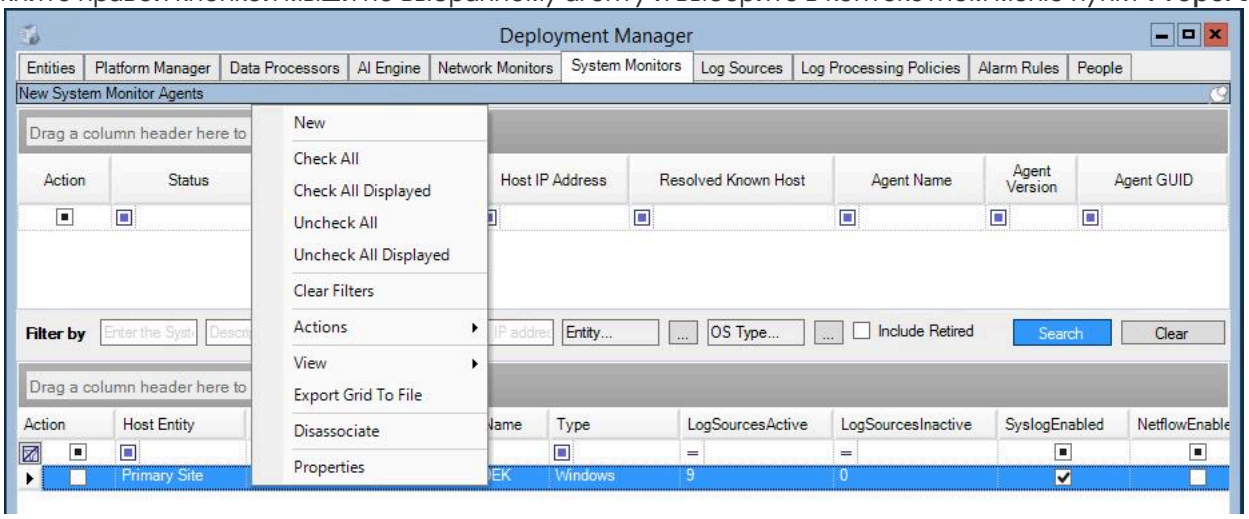
В этом разделе описаны действия, которые необходимо выполнить, чтобы новый источник журналов, относящийся к Kaspersky CyberTrace, появился в LogRhythm. Если LogRhythm уже настроен должным образом, дополнительные действия не требуются, поскольку новый источник журналов появится в LogRhythm и достаточно проверить, все ли работает в соответствии с требованиями.

Чтобы создать условия для добавления источника журнала, относящегося к Kaspersky CyberTrace, в LogRhythm, выполните следующие действия:

1. Запустите LogRhythm Console.

2. Выберите **Deployment Manager** → **System Monitors**.

3. Щелкните правой кнопкой мыши по выбранному агенту и выберите в контекстном меню пункт **Properties**.

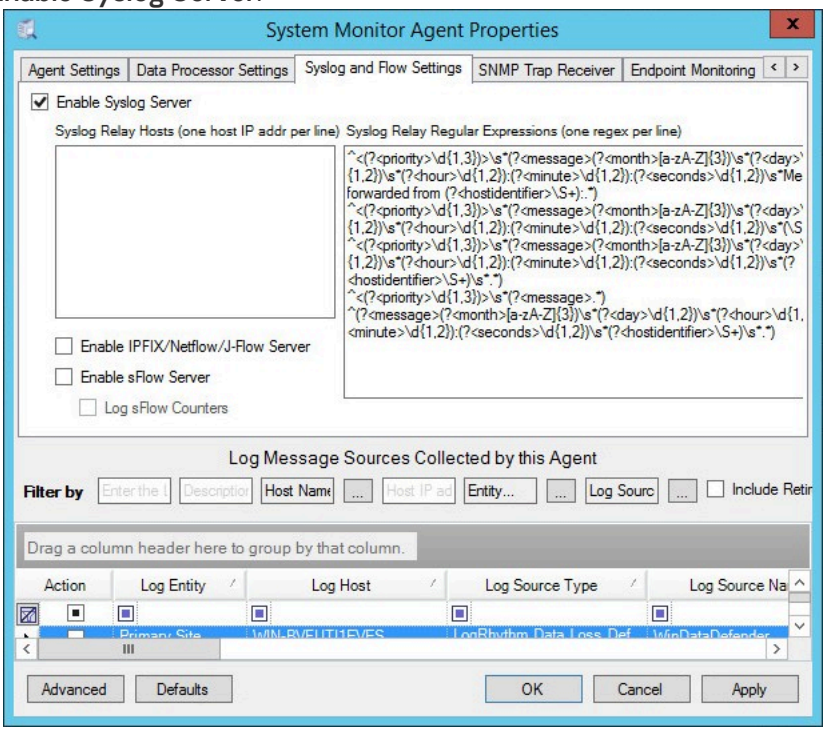


Контекстное меню агента

Откроется окно **System Monitor Agent Properties**.

4. Выберите вкладку **Syslog and Flow Settings**.

5. Установите флажок **Enable Syslog Server**.



Окно **System Monitor Agent Properties**

6. Нажмите на кнопку **OK**.

7. Выключите Брандмауэр Windows или добавьте в него исключения, чтобы разрешить поступление входящих событий SYSLOG.

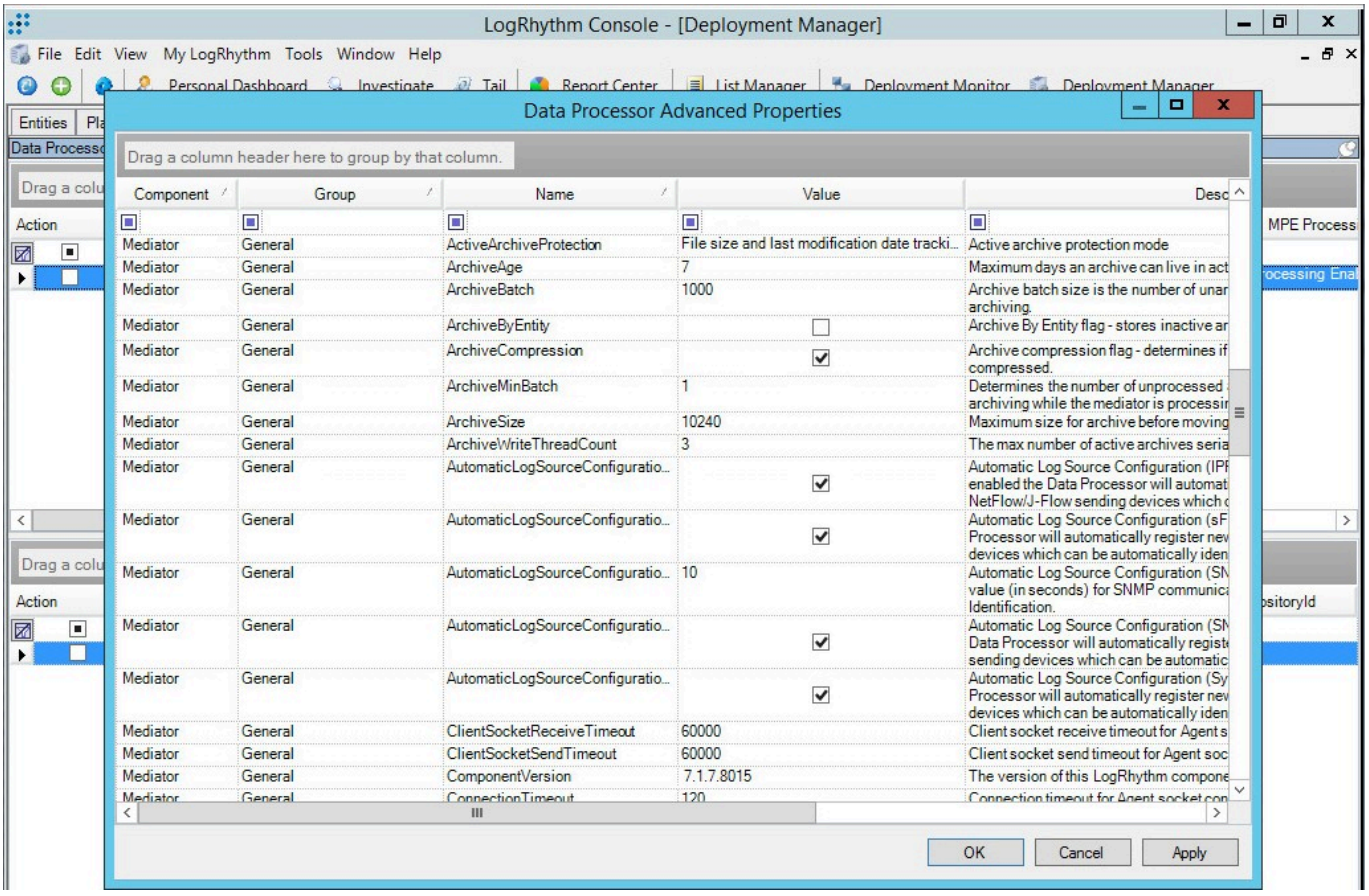
8. Выберите **Deployment Manager** → **Data Processors** → **Properties** → **Advanced**.

   Откроется окно **Data Processor Advanced Properties**.

9. В таблице выберите следующие элементы. Имена свойств содержатся в столбце **Name**, а в столбце **Value** содержатся флажки, которые необходимо установить:

   - AutomaticLogSourceConfigurationNetFlow
   - AutomaticLogSourceConfigurationsFlow

- AutomaticLogSourceConfigurationSNMPTrap
- AutomaticLogSourceConfigurationSyslog



Окно **Data Processor Advanced Properties**

10. Нажмите на кнопку **OK**.
11. При необходимости перезапустите LogRhythm.

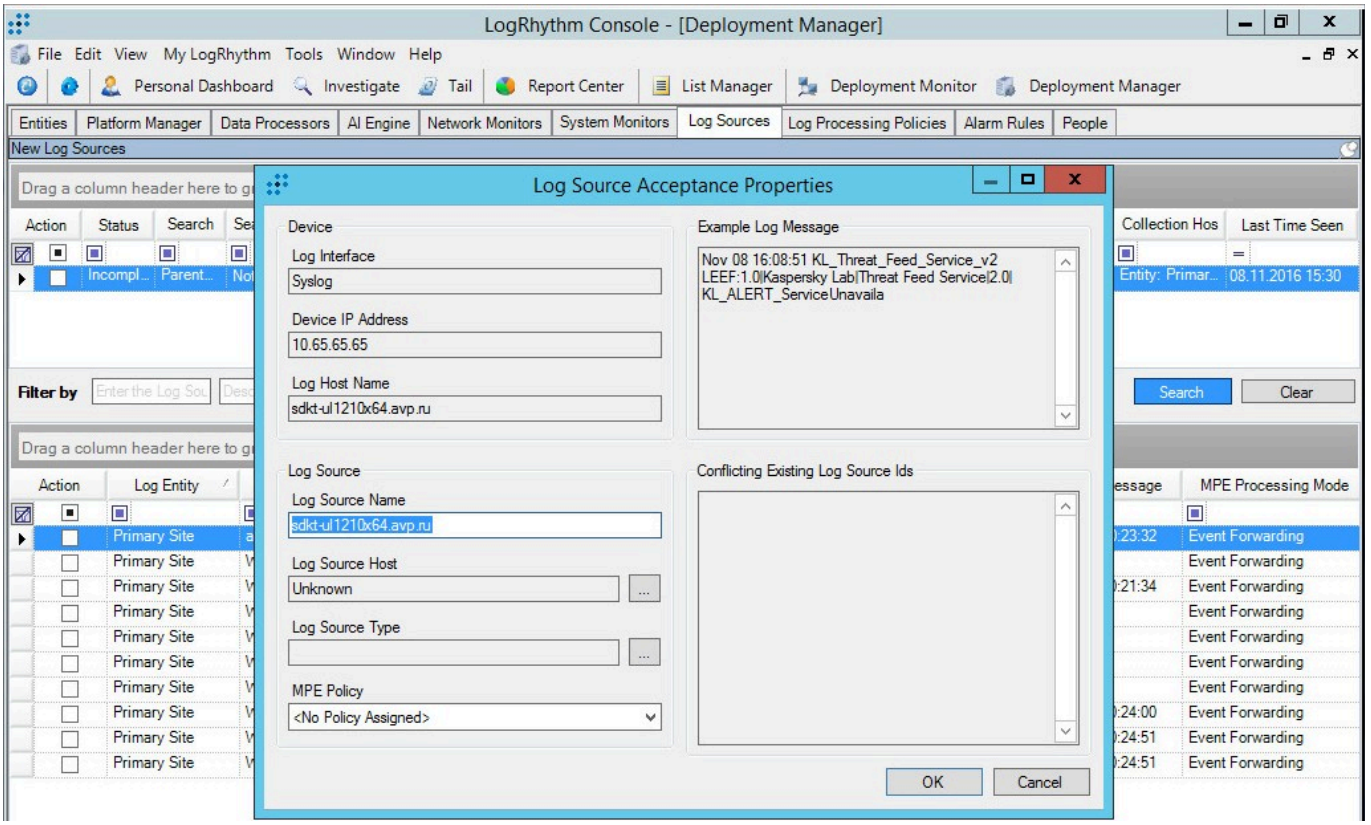
    LogRhythm сообщит, требуется ли перезагрузка.

После того, как Kaspersky CyberTrace отправит событие, на вкладке **Log Sources** появится новый элемент.

Чтобы принять новый источник журнала, выполните следующие действия:

1. Щелкните по новому элементу правой кнопкой мыши и выберите пункт контекстного меню **Actions → Resolve Log Source Hosts**.
2. Дважды щелкните по новому элементу.

Откроется окно **Log Source Acceptance Properties**.



Окно **Log Source Acceptance Properties**

3. Измените свойства:

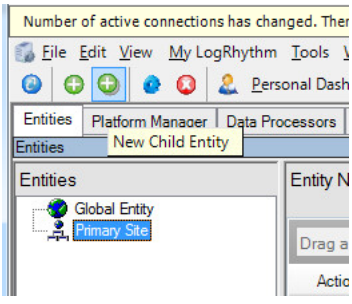
   - Укажите хост источника журналов.
   - В качестве типа источника журналов укажите `Kaspersky CyberTrace`.
   - Укажите политику MPE, добавленную на шаге 4.

4. Нажмите на кнопку **OK**.

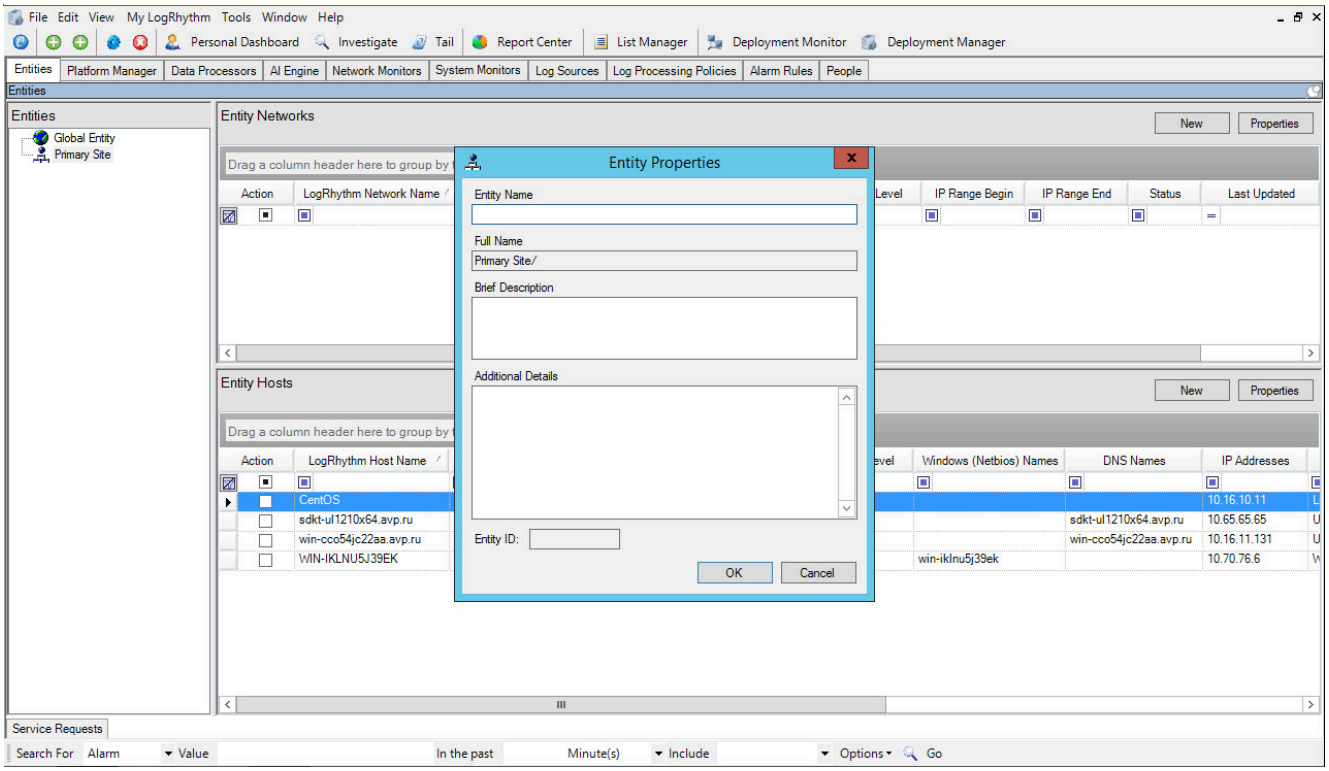
5. Если выводится сообщение об ошибке, указывающее на невозможность использования неизвестного хоста источника журналов, добавьте новую сущность следующим образом:

   a. В LogRhythm Console выберите вкладку **Entities**.

   b. Нажмите на кнопку **New Child Entity** на панели инструментов.



   c. В открывшемся окне **Entity Properties** задайте свойства объекта.



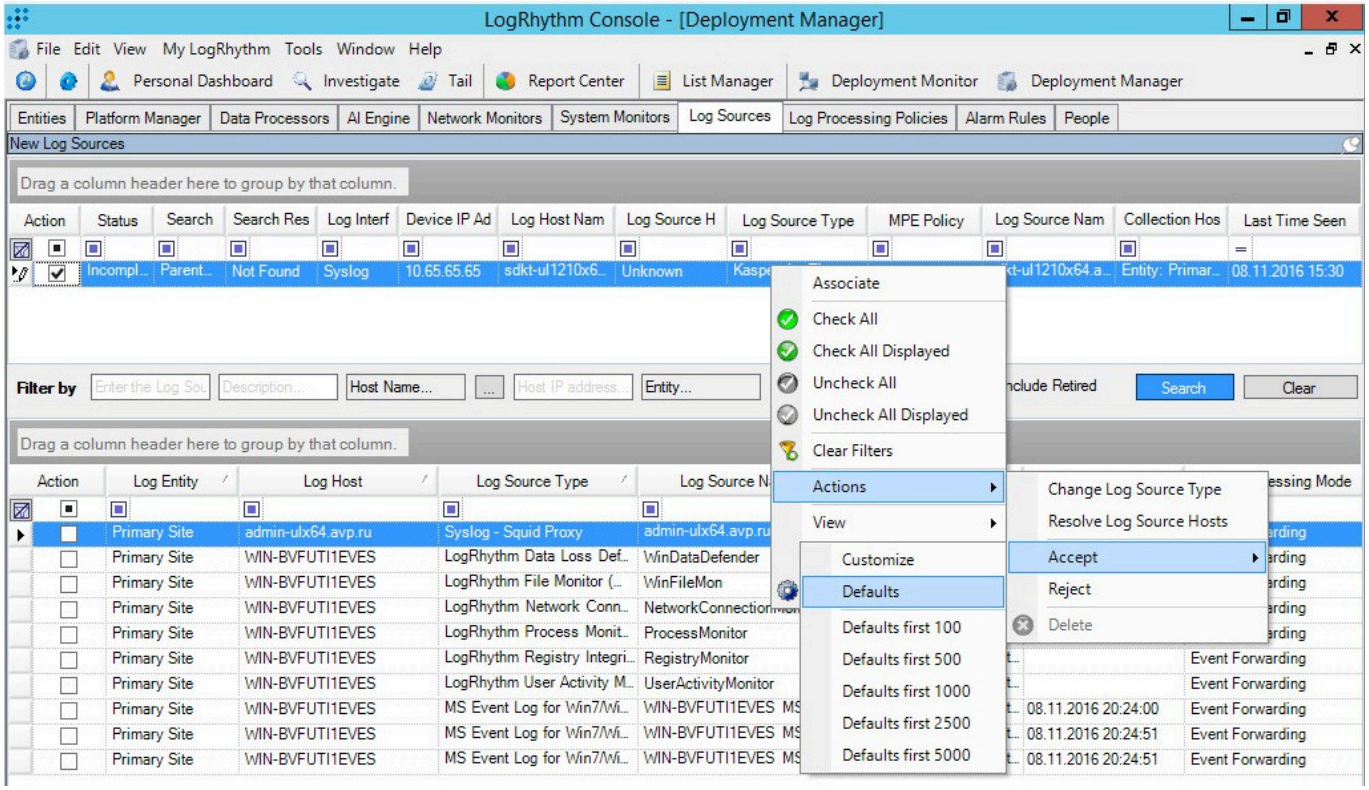
Имя сущности должно быть уникальным и не может быть пустым. Остальные свойства сущности могут быть произвольными.

d. Нажмите на кнопку **OK**.

e. Повторите действие на шаге 3, используя созданную сущность в качестве хоста источника журнала.

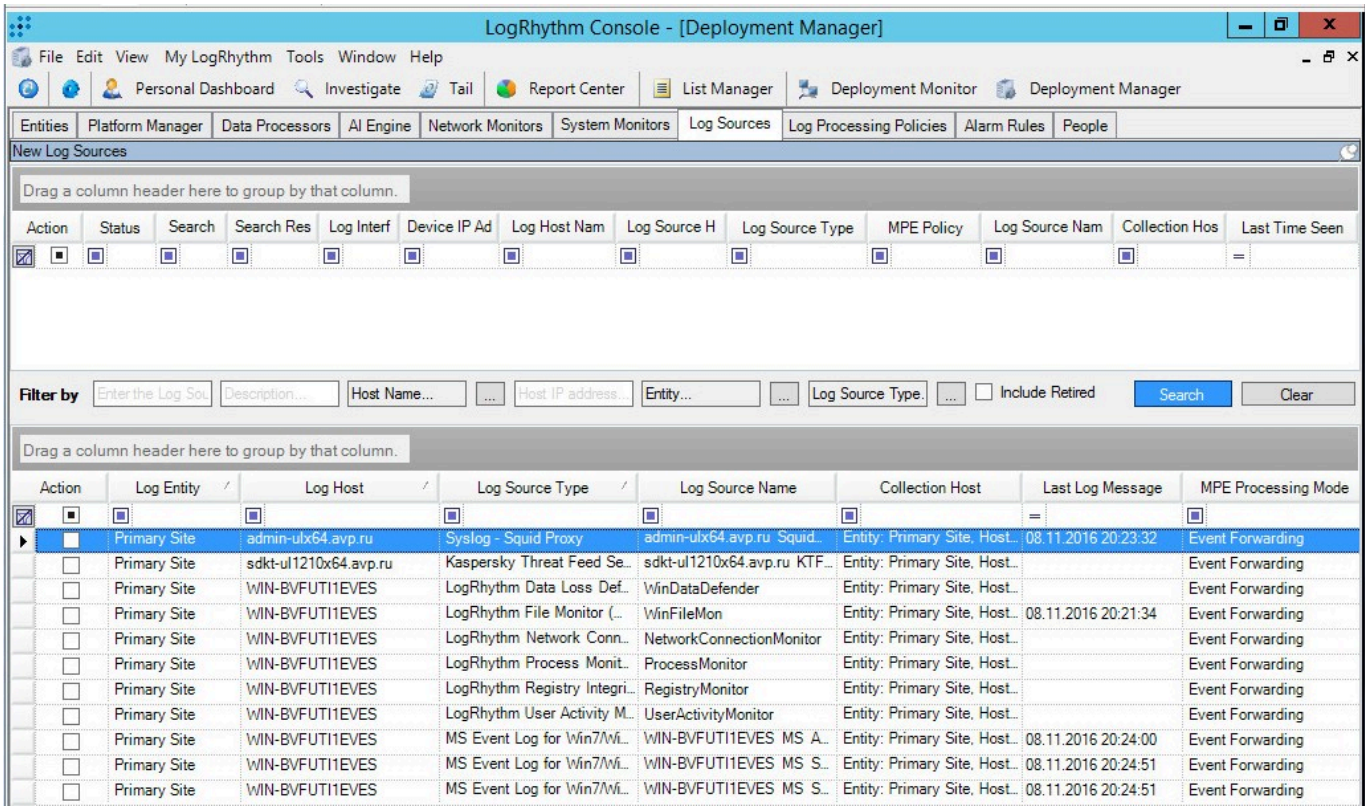
6. Установите флажок **Action**.

7. Щелкните правой кнопкой мыши по источнику журналов и выберите **Actions** → **Accept** → **Defaults**.



Контекстное меню источника журналов

В нижней таблице LogRhythm Console отобразится новый источник журналов.



Новый источник журналов

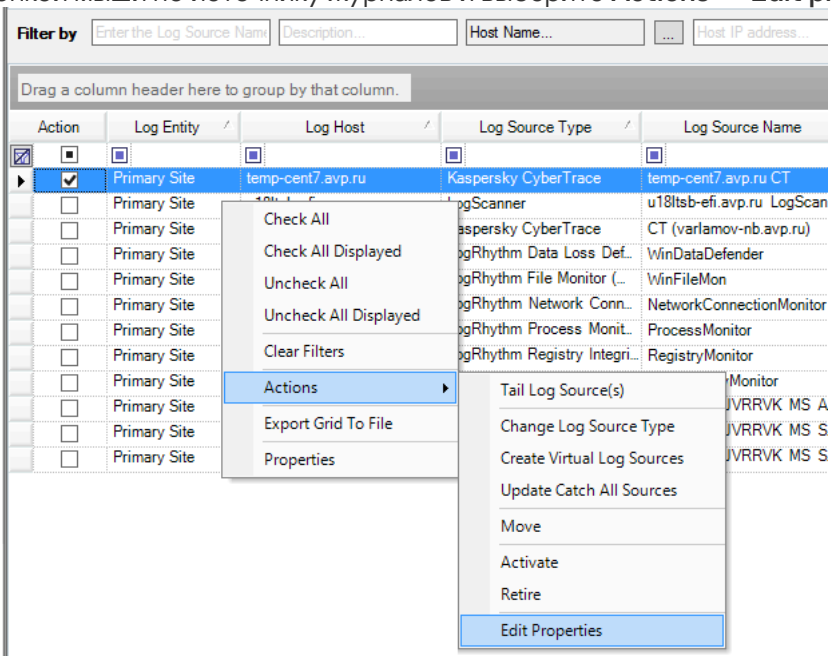
Отключение пересылки журналов для событий, получаемых от Kaspersky CyberTrace

Отключение пересылки журналов для событий, получаемых из Kaspersky CyberTrace, может потребоваться для исключения зацикливания событий, т. е. пересылки полученных событий обратно в Kaspersky CyberTrace.

Чтобы отключить пересылку журналов для событий, получаемых от Kaspersky CyberTrace, выполните следующие действия:

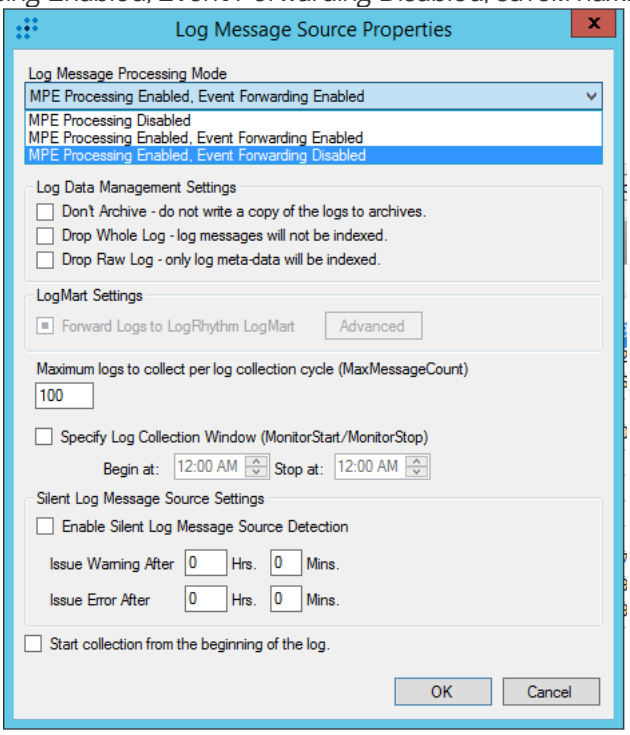
1. На вкладке **Log Sources** установите флажок для источника журналов, связанного с Kaspersky CyberTrace.

2. Щелкните правой кнопкой мыши по источнику журналов и выберите **Actions** → **Edit properties**.



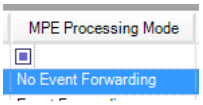
Изменение свойств источника журналов **Kaspersky CyberTrace**

3. Откроется окно **Log Message Source Properties**. В раскрывающемся списке **Log Message Processing Mode** выберите *MPE Processing Enabled, Event Forwarding Disabled*, затем нажмите на кнопку **OK**.



Указание режима обработки журналов

В столбце **MPE Processing Mode** для выбранного источника журналов отображается *No Event Forwarding*.



Столбец **MPE Processing Mode**

Шаг 7. Настройка пересылки журналов в Kaspersky CyberTrace

В этом разделе рассматривается порядок настройки LogRhythm для пересылки журналов в Kaspersky CyberTrace. Настройка LogRhythm включает добавление приемника журналов и добавление политики рассылки журналов.

Добавление приемника журналов

Создайте новый приемник журналов в LogRhythm. Этот приемник журналов будет представлять Kaspersky CyberTrace.

Чтобы добавить приемник журналов в LogRhythm, выполните следующие действия:

1. Запустите LogRhythm Console.
2. Выберите **Deployment Manager** → **Tools** → **Distribution** → **Log Distribution Services** → **Receiver Manager**.
   Откроется окно **Log Distribution Receiver Manager**.
3. Выберите **File** → **New**.

4. Заполните поля открывшегося окна **Syslog Receiver Properties**:

   - Укажите IP-адрес удаленного хоста, на котором установлено приложение Kaspersky CyberTrace (IP-адрес, указанный в элементе `InputSettings > ConnectionString` конфигурационного файла Kaspersky CyberTrace Service).
   - Укажите удаленный порт, который Kaspersky CyberTrace прослушивает для получения событий (порт, указанный в элементе `InputSettings > ConnectionString` конфигурационного файла Kaspersky CyberTrace Service).
   - Измените значение параметра **Network Protocol** на «TCP».
   - Снимите флажок **Сократить сообщение до 1024 байтов (RFC 3164)**.

5. Нажмите на кнопку **OK**.

6. После появления новой строки в таблице, щелкните по ней правой кнопкой мыши и выберите пункт контекстного меню **Enable**.

Добавление политики рассылки журналов

После добавления приемника журналов задайте условия путем добавления политики рассылки журналов для событий, которые будут пересылаться в Kaspersky CyberTrace.

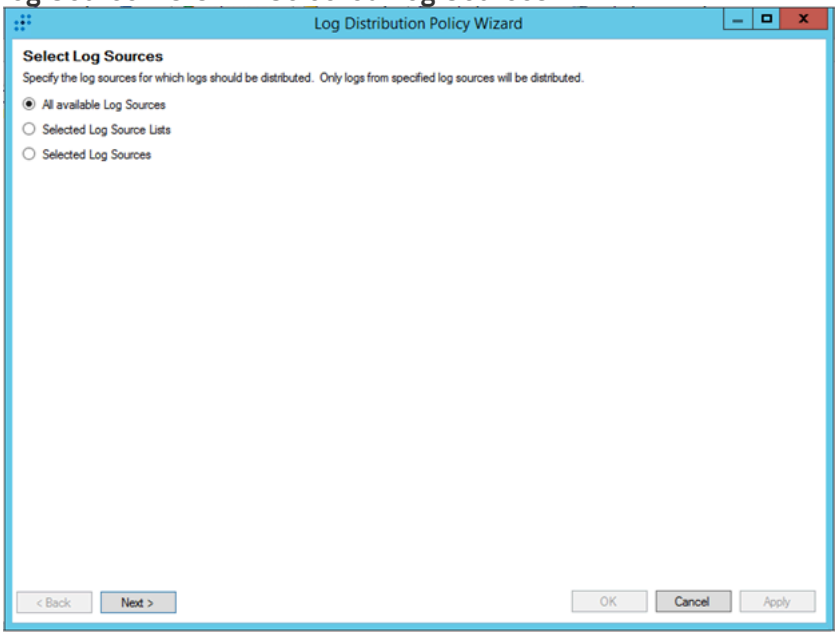
Чтобы добавить политику рассылки журналов, выполните следующие действия:

1. Выберите **Deployment Manager** → **Tools** → **Distribution** → **Log Distribution Services** → **Policy Manager**.

2. В открывшемся окне **Log Distribution Policy Manager** выберите **File** → **New**.

   Запустится мастер Log Distribution Policy Wizard. Пройдите следующие шаги мастера, нажимая на кнопку **Next**.

3. Выберите **Selected Log Source Lists** или **Selected Log Sources**.



Окно Select Log Sources

4. В открывшемся окне воспользуйтесь фильтром и укажите источники журналов для событий, которые требуется пересылать в Kaspersky CyberTrace.

   Убедитесь, что Kaspersky CyberTrace не выбран в качестве источника журналов для пересылки, поскольку это привело бы к зацикливанию событий. По той же причине не следует выбирать **All available Log Sources** на предыдущем шаге.

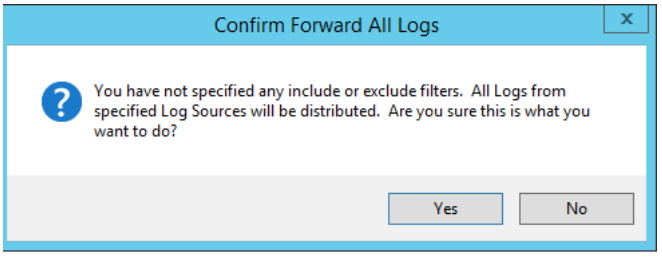
5. В окне **Event Distribution Criteria** можно задать более точные фильтры для источников журналов, указанных на предыдущем шаге.

   Дополнительные сведения об определении этих фильтров приведены в документации LogRhythm.

   Рекомендуется не указывать эти фильтры.

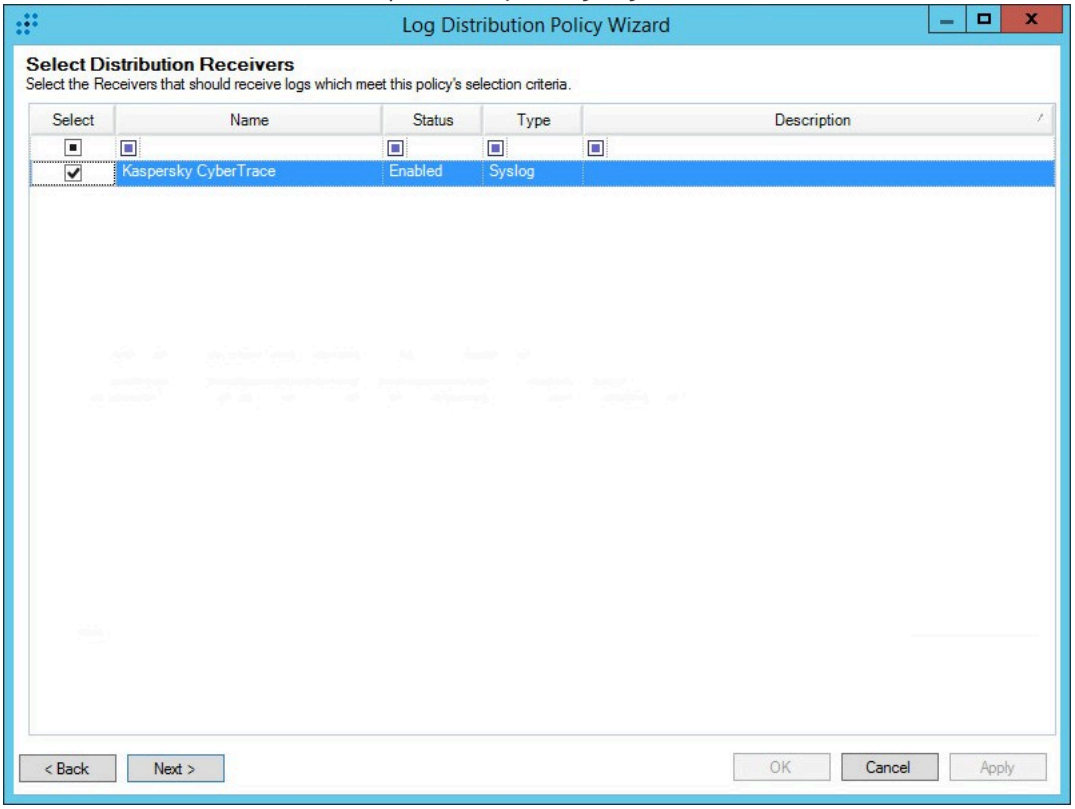
6. Если на предыдущем шаге не были указаны какие-либо фильтры, откроется окно подтверждения, как показано на рисунке ниже.

   Нажмите на кнопку **Yes**.



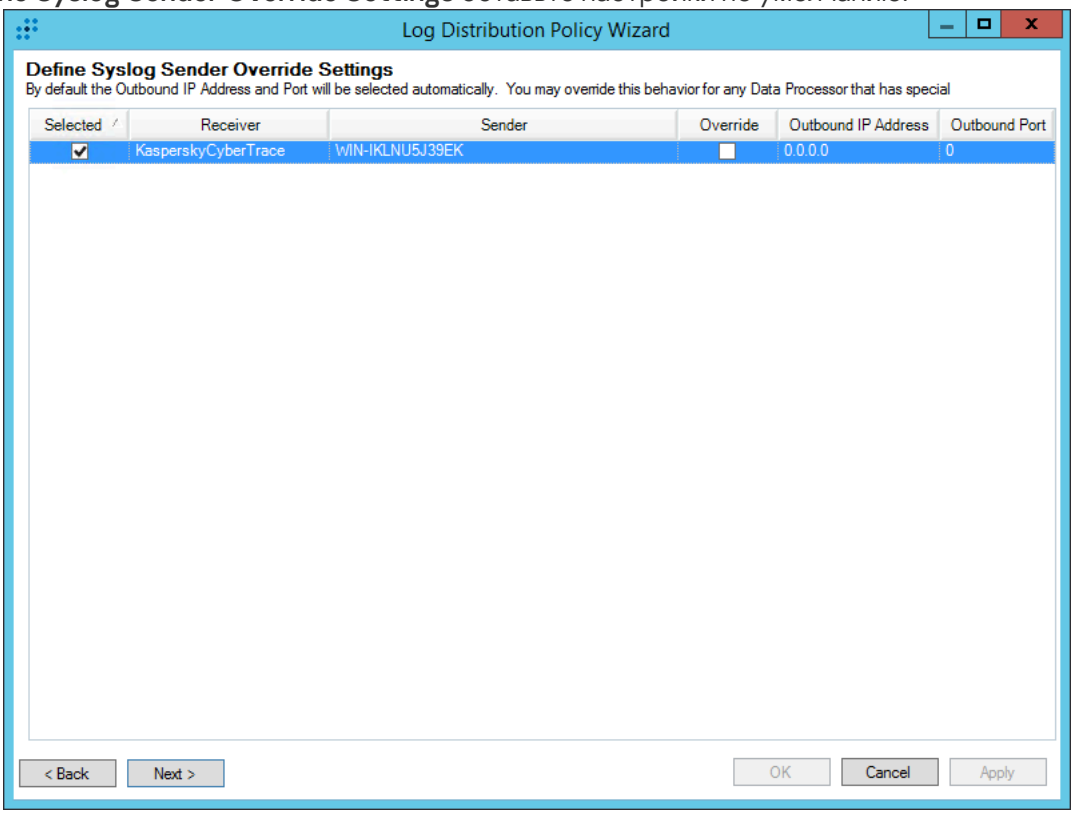
Подтверждение пересылки всех журналов без применения фильтров

7. В окне **Select Distribution Receivers** выберите `Kaspersky CyberTrace`.



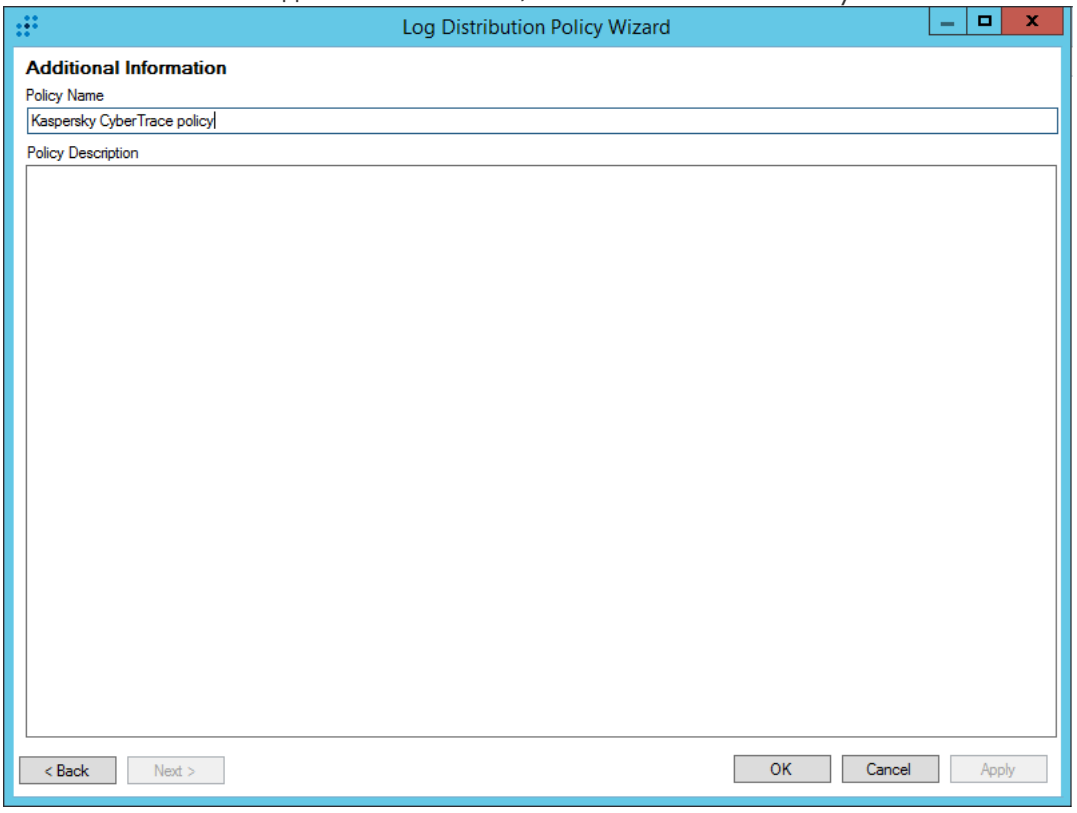
Окно **Select Distribution Receivers**

8. В окне **Define Syslog Sender Override Settings** оставьте настройки по умолчанию.



Окно **Define Syslog Sender Override Settings**

9. В окне **Additional Information** введите имя политики, затем нажмите на кнопку **OK**.



Окно **Additional Information**

10. После завершения работы мастера **Log Distribution Policy Wizard** в таблице появится новая строка.

    Щелкните правой кнопкой мыши по новой строке в таблице и выберите пункт контекстного меню **Enabled**.

Сервер, на котором установлено приложение Kaspersky CyberTrace, начнет получать журналы. Это можно проверить с помощью утилиты netcat.

Отображение событий обнаруженных киберугроз в LogRhythm

В результате вышеуказанных действий LogRhythm начнет получать и отображать события обнаруженных киберугроз. События также будут отображаться в веб-консоли, доступной по адресу `https://<logrhythmIP>:8443` или `https://<logrhythmIP>:80`.

Шаг 8. Проверка работоспособности

В этом разделе описывается порядок проверки правильности интеграции Kaspersky CyberTrace с LogRhythm путем выполнения проверки работоспособности.

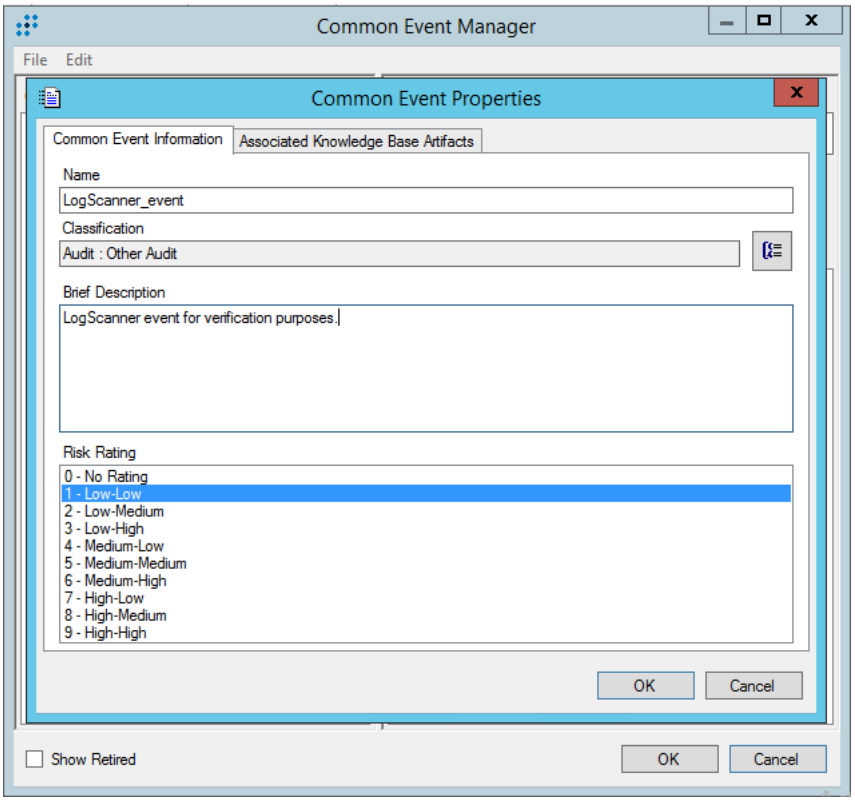
Чтобы создать условия для проведения проверки работоспособности:

1. Создайте пользовательский тип источника журналов, как описано в разделе Шаг 1. Добавление пользовательского типа источника журналов, со следующими параметрами:

Поле	Данные
Имя	Kaspersky LogScanner
Full Name	Kaspersky LogScanner
Abbreviation	LogScanner
Log Format	Syslog
Brief Description	Kaspersky LogScanner is a command-line application that allows you to send data to Kaspersky CyberTrace Service for checking against feeds.

2. Добавьте новое общее событие, как описано в разделе Шаг 3 (необязательный). Добавление событий Kaspersky CyberTrace, со следующими параметрами:

Поле	Данные
Имя	LogScanner_event
Classification	Audit : Other Audit
Brief Description	LogScanner event for verification purposes
Risk Rating	Low-Low

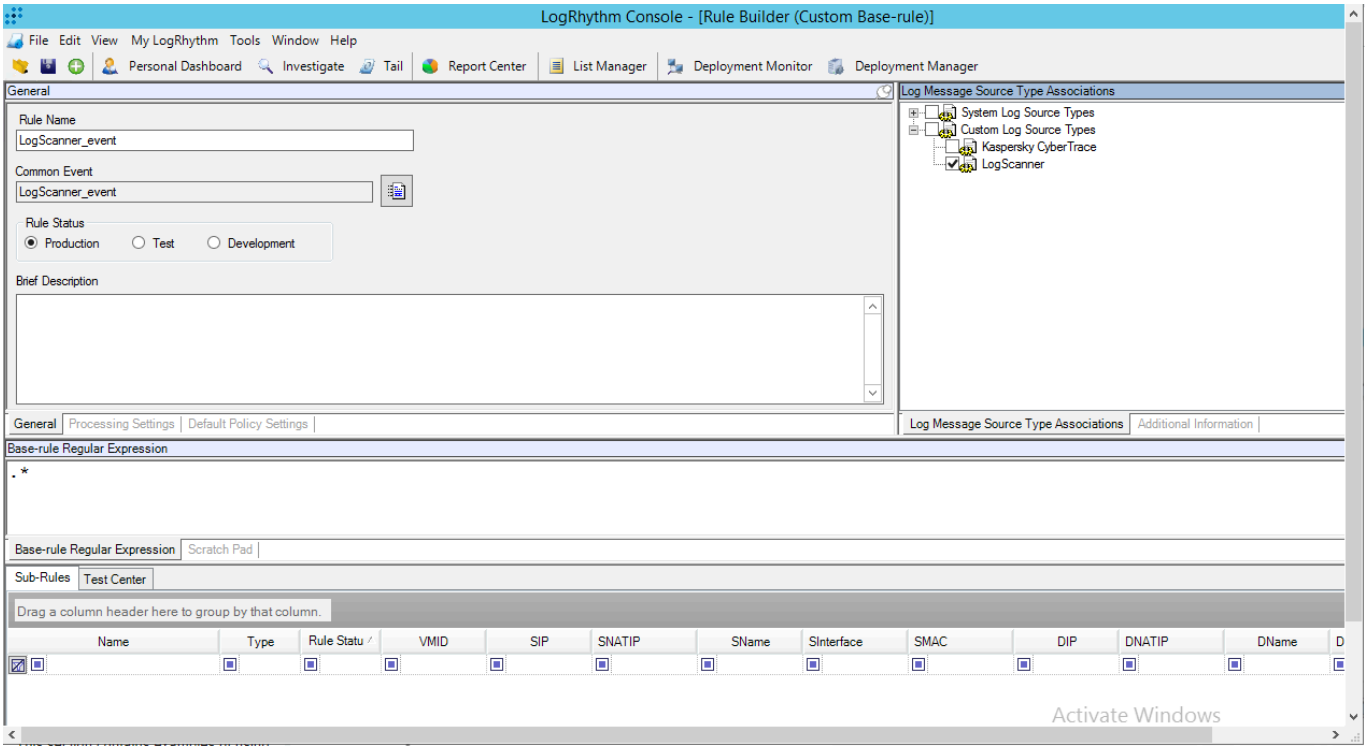


Окно **Common Event Properties**

3. Добавьте правило MPE для Log Scanner, как описано в разделе Шаг 4 (необязательный). Добавление правил Kaspersky CyberTrace, со следующими параметрами:

   - На панели дерева **Log Message Source Type Associations** выберите **Kaspersky LogScanner**.
   - Укажите `LogScanner_event` в качестве имени правила (**Rule Name**).
   - В раскрывающемся списке **Common Event** выберите **LogScanner_event**.

- В поле **Rule Status** выберите **Production**.
- В поле **Base-Rule Regular Expression** введите «`.*`».



Форма конструктора правил

4. Создайте новую политику для Kaspersky Log Scanner, как описано в разделе Шаг 5. Добавление политики Kaspersky CyberTrace.

   В списке **Log Source Type** выберите **Kaspersky LogScanner**. Задайте все остальные параметры, как описано в разделе Шаг 5. Добавление политики Kaspersky CyberTrace.

5. Добавьте источник журналов в System Monitor Agent:

   a. В файле конфигурации Log Scanner укажите IP-адрес сервера, на котором работает LogRhythm, и порт `514`.

   b. Отправьте файл `%service_dir%/verification/kl_verification_test_cef.txt` в LogRhythm.

   - Для этого выполните следующую команду (в Linux):

     ```
     ./log_scanner -p ../verification/kl_verification_test_cef.txt
     ```

   - Для этого выполните следующую команду (в Windows):

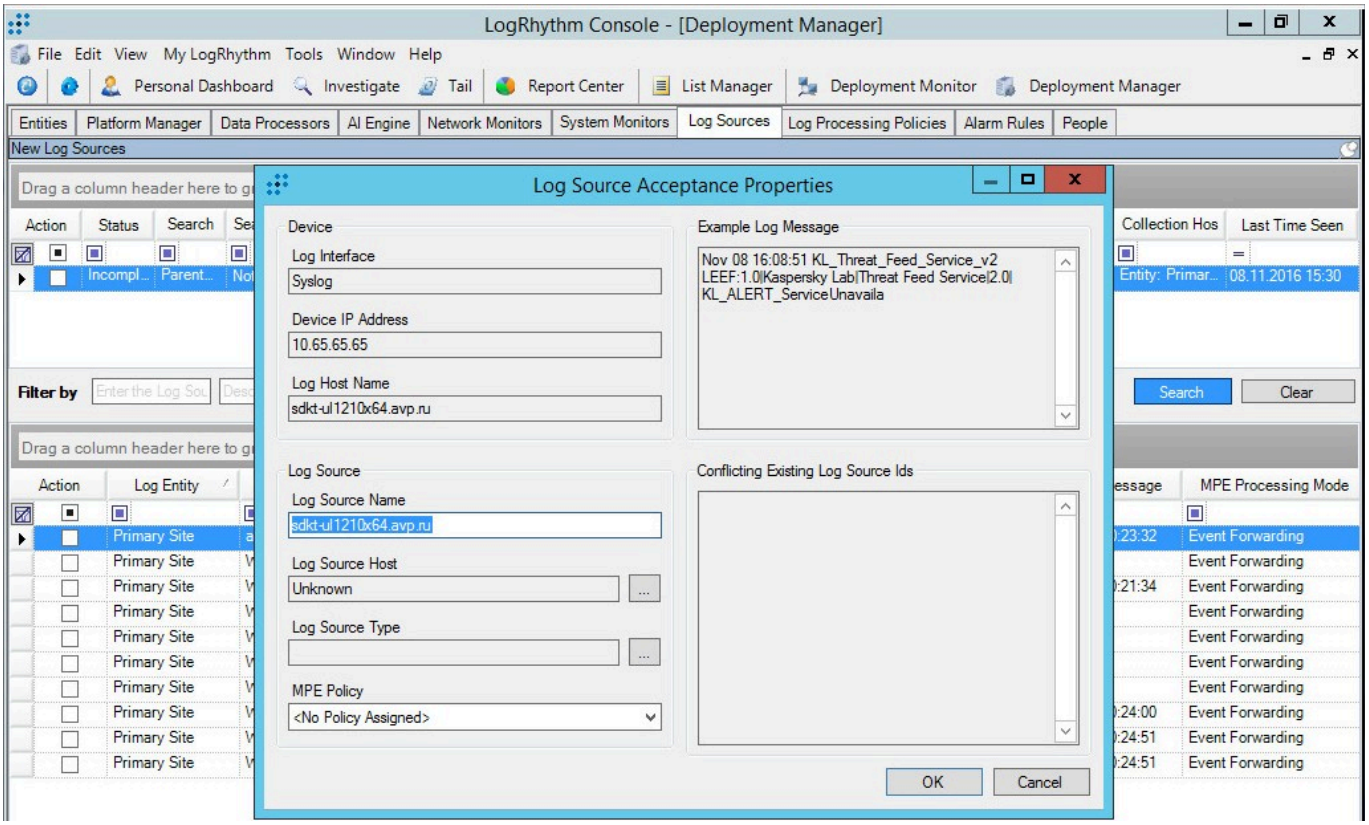
     ```
     log_scanner.exe -p ..\verification\kl_verification_test_cef.txt
     ```

После того, как Kaspersky Log Scanner отправит событие, на вкладке **Log Sources** появится новый элемент.

Чтобы принять новый источник журнала, выполните следующие действия:

1. Щелкните по новому элементу правой кнопкой мыши и выберите пункт контекстного меню **Actions** → **Resolve Log Source Hosts**.
2. Дважды щелкните по новому элементу.

Откроется окно **Log Source Acceptance Properties**.



Окно **Log Source Acceptance Properties**

3. Измените свойства:

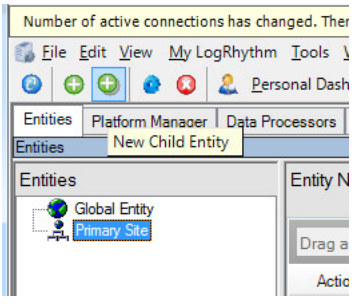
   - Укажите хост источника журналов.
   - Укажите `Kaspersky LogScanner` в качестве типа источника журналов.
   - Выберите политику MPE, созданную ранее для Kaspersky Log Scanner.

4. Нажмите на кнопку **OK**.

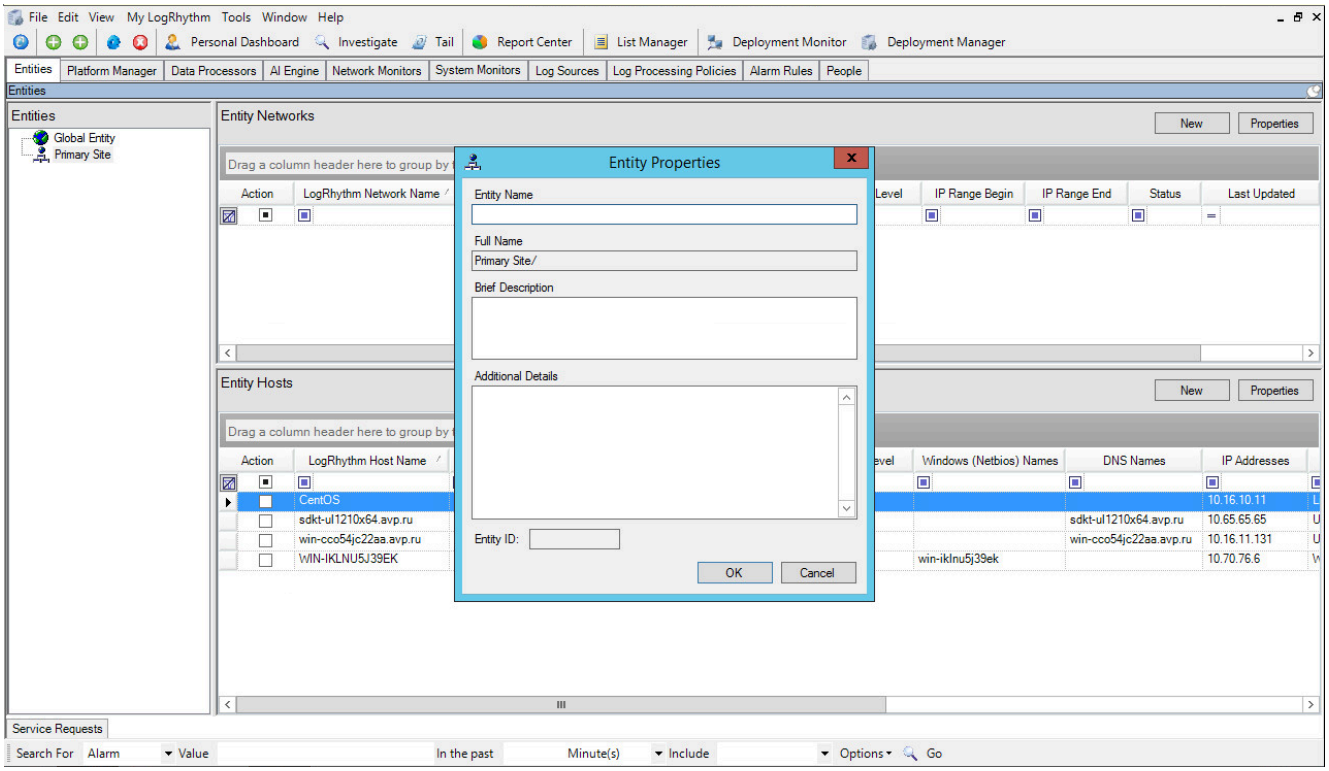
5. Если выводится сообщение об ошибке, указывающее на невозможность использования неизвестного хоста источника журналов, добавьте новую сущность следующим образом:

   a. В LogRhythm Console перейдите на вкладку **Entities**.

   b. Нажмите на кнопку **New Child Entity** на панели инструментов.



   c. В открывшемся окне **Entity Properties** задайте свойства объекта.



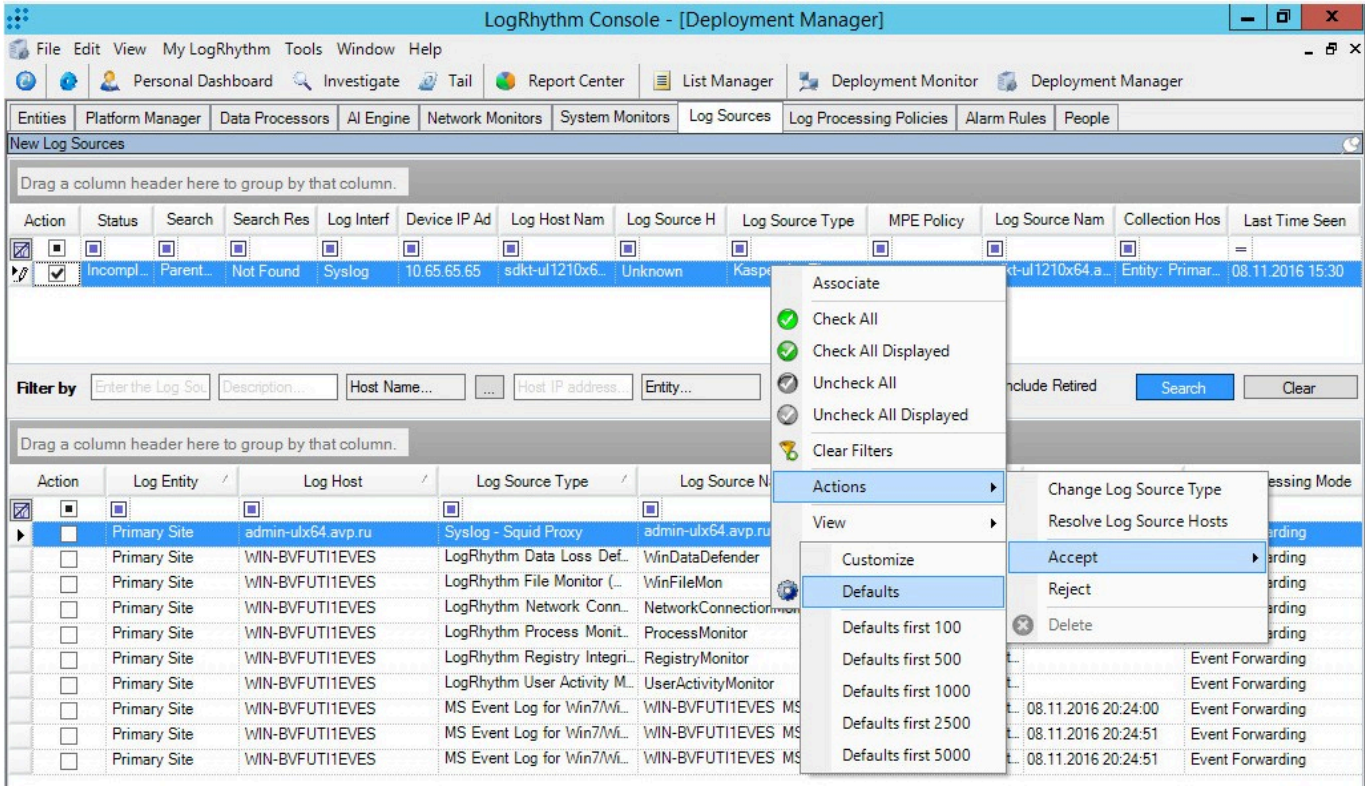
Имя сущности должно быть уникальным и не может быть пустым. Остальные свойства сущности могут быть произвольными.

d. Нажмите на кнопку **OK**.

e. Повторите действие на шаге 3, используя созданную сущность в качестве хоста источника журнала.

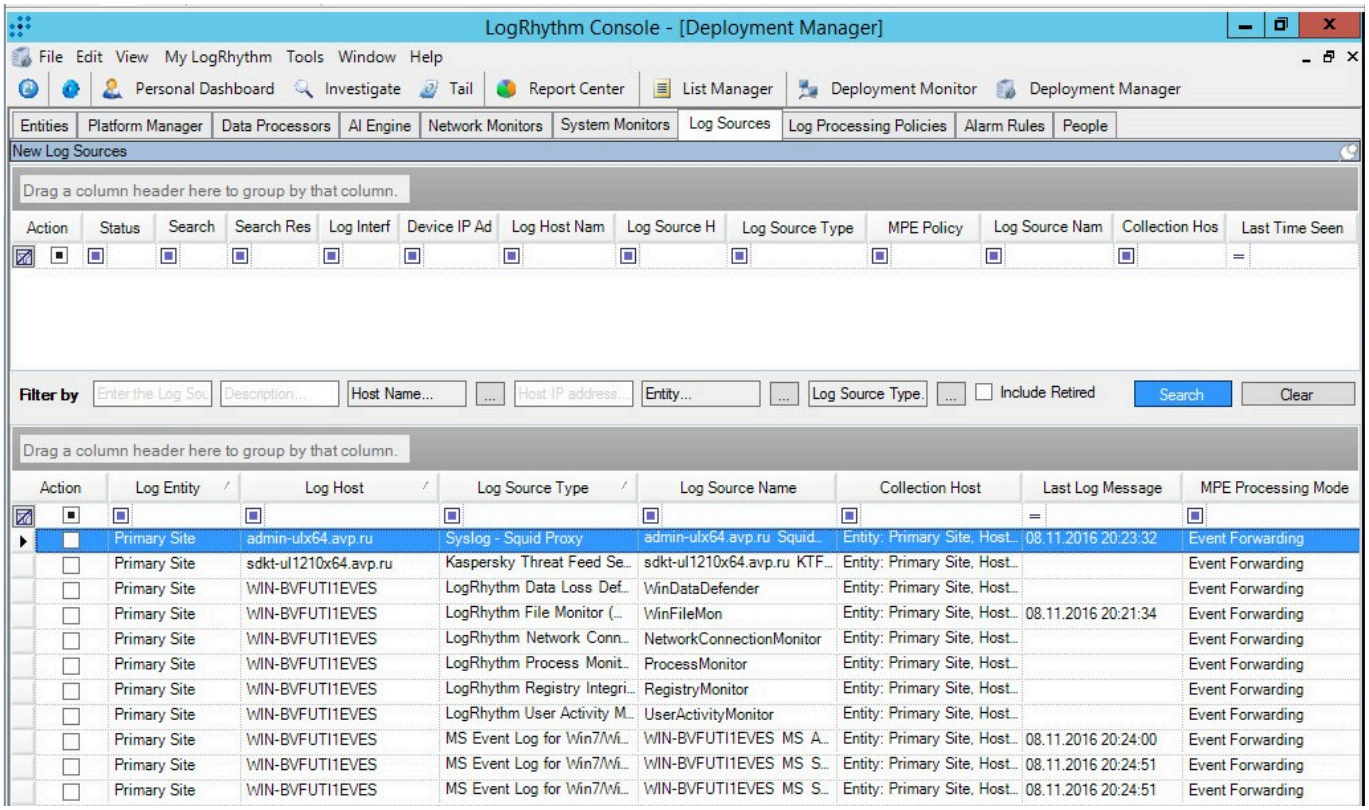
6. Установите флажок **Action**.

7. Щелкните правой кнопкой мыши по источнику журналов и выберите **Actions** → **Accept** → **Defaults**.



Контекстное меню источника журналов

В нижней таблице LogRhythm Console отобразится новый источник журналов.



Новый источник журналов

8. Перезагрузите LogRhythm.

Если ранее была настроена пересылка журналов, как описано в разделе Шаг 7. Настройка пересылки журналов в Kaspersky CyberTrace, убедитесь, что **Kaspersky LogScanner** выбран в качестве источника журналов (**Log source**) (см. подраздел «Добавление политики рассылки журналов»).

Чтобы выполнить проверку работоспособности, выполните следующие действия:

Повторно отправьте файл `%service_dir%/verification/kl_verification_test_cef.txt` в LogRhythm.

- Для этого выполните следующую команду (в Linux):

  ```
  ./log_scanner -p ../verification/kl_verification_test_cef.txt
  ```

- Для этого выполните следующую команду (в Windows):

  ```
  log_scanner.exe -p ..\verification\kl_verification_test_cef.txt
  ```

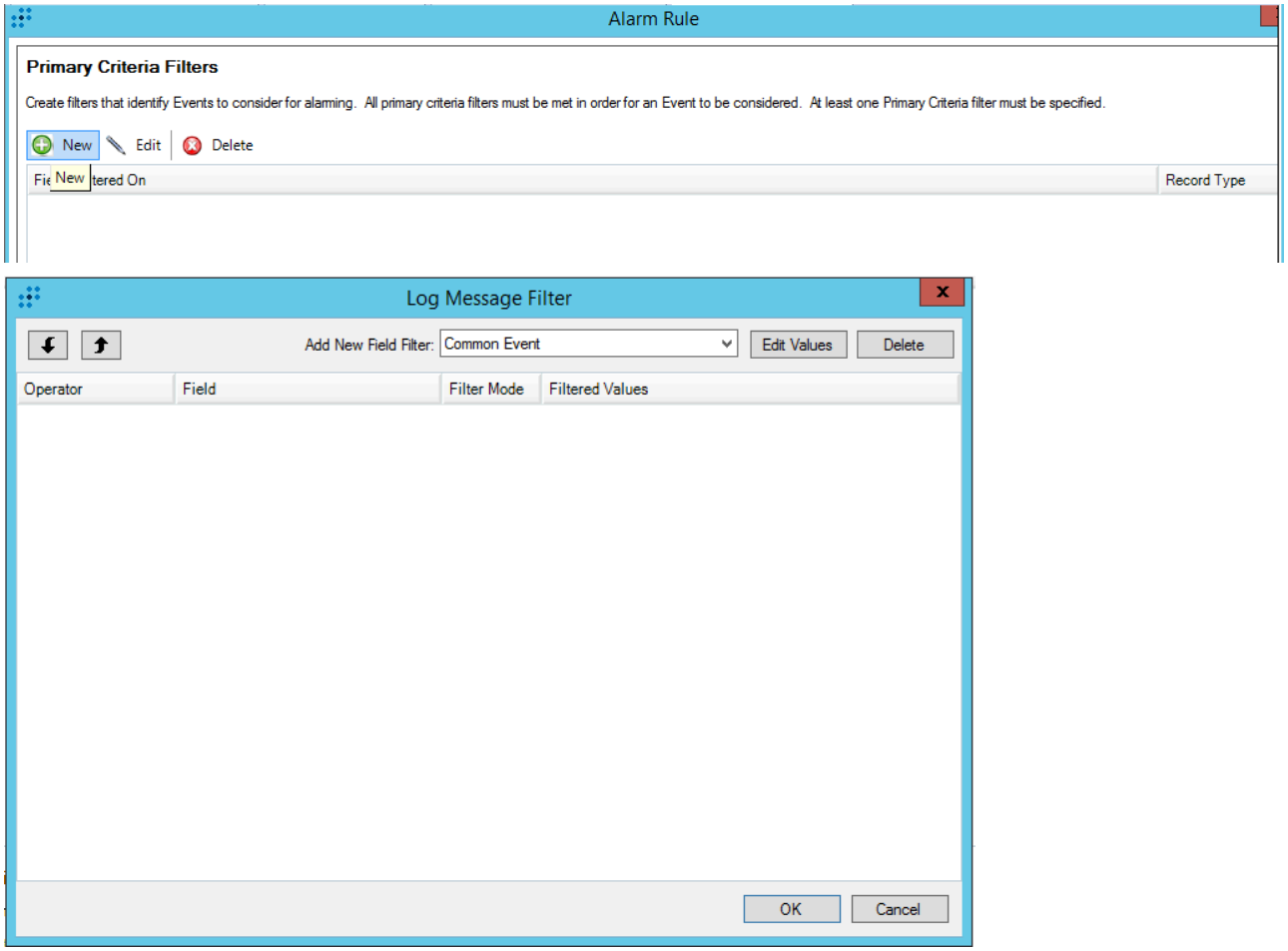
Если интеграция Kaspersky CyberTrace с LogRhythm настроена правильно, тестовые события из Log Scanner будут автоматически пересылаться в Kaspersky CyberTrace. После этого оповещения о событии из Kaspersky CyberTrace будут отправляться в LogRhythm. Количество оповещений может варьироваться в зависимости от включенных потоков данных об угрозах Kaspersky Threat Data Feeds. Оповещения о событиях могут отображаться в веб-консоли LogRhythm, как описано в разделе Шаг 10 (необязательный). Отображение оповещений о событиях в LogRhythm. Также можно проверить интеграцию с LogRhythm, создав очередь отображения исходных событий в реальном времени на вкладке **Tail** консоли LogRhythm.

Шаг 9 (необязательный). Создание информационных сообщений о входящих служебных событиях Kaspersky CyberTrace

Для создания уведомлений о входящих служебных событиях Kaspersky CyberTrace можно настроить правила оповещений.

Чтобы создать уведомления о служебных событиях из Kaspersky CyberTrace в LogRhythm, выполните следующие действия:

1. Запустите LogRhythm Console.
2. Выберите **Deployment Manager** → **Alarm Rules** и нажмите **New**.
3. В окне подтверждения **Create Global Rule** нажмите кнопку **Yes**, если требуется предоставить доступ к работе с этим правилом всем пользователям, у которых есть роль **Global Admin**. Нажмите **No**, если с этим правилом должен работать только текущий пользователь.
4. Выполните следующие действия на каждой вкладке внизу страницы:
   - На вкладке **Primary Criteria**:
     1. Нажмите кнопку **New** и выберите значение **Common Event** в раскрывающемся списке **Add New Field Filter**.

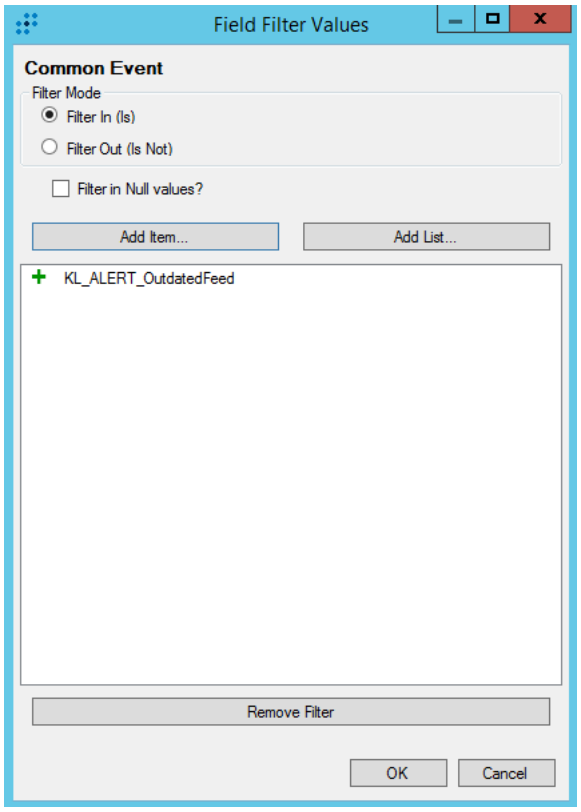


     2. Нажмите на кнопку **Edit values**.

        Откроется окно **Field Filter Values**.

3. В окне **Field Filter Values** нажмите на кнопку **Add Item**.

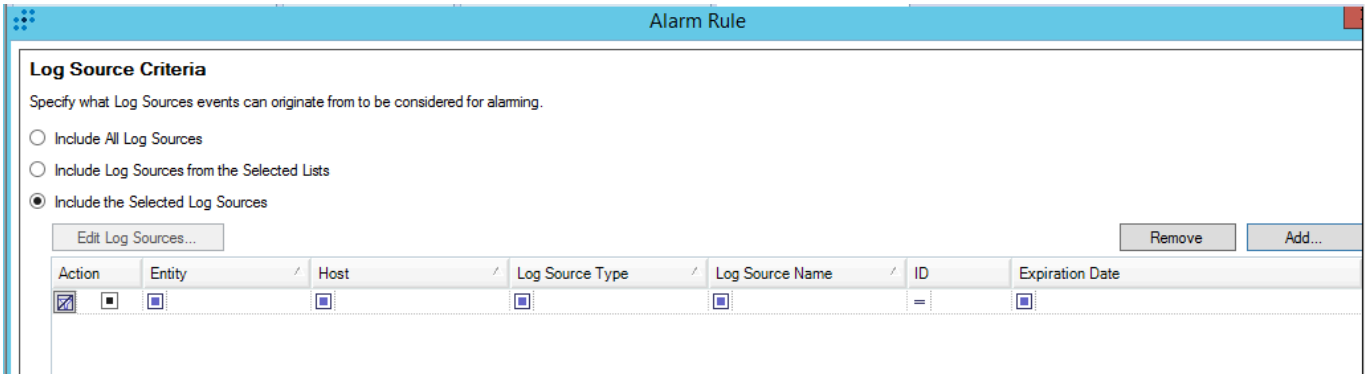
4. Выберите имя служебного события Kaspersky CyberTrace из списка. Если такие события отсутствуют, добавьте их, как описано в разделе Добавление событий Kaspersky CyberTrace.



5. Нажмите на кнопку **OK**.

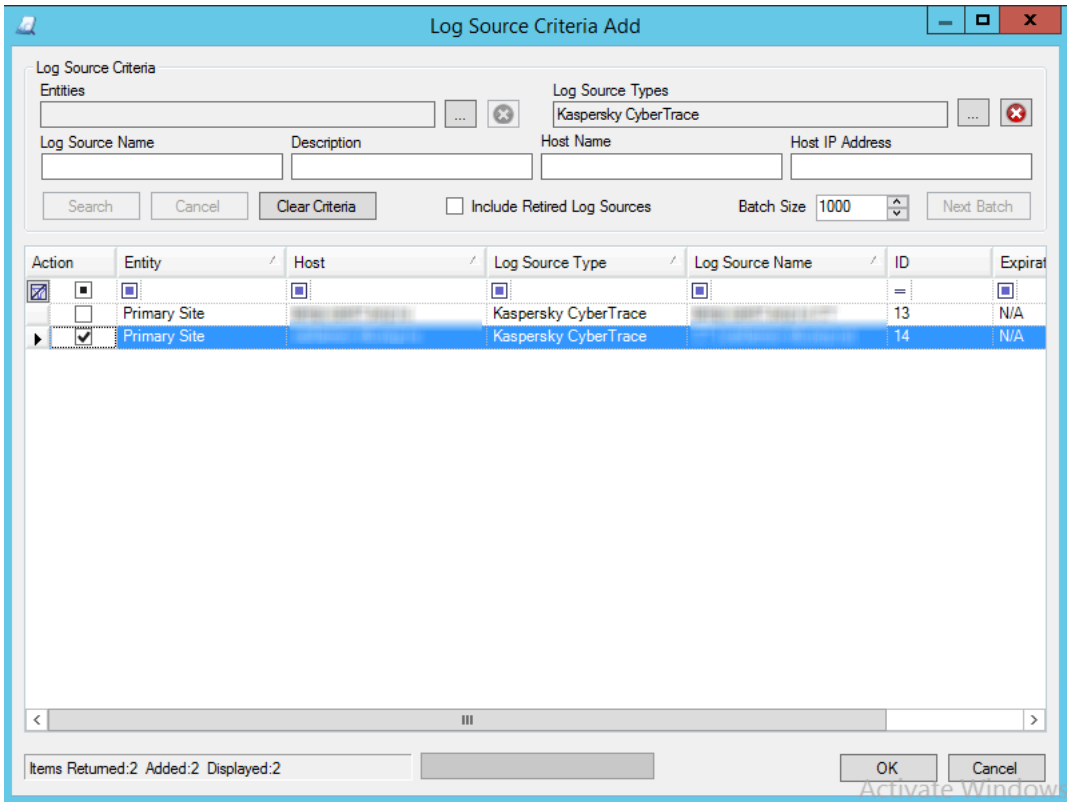
- Оставьте вкладки **Include Filters**, **Exclude Filters** и **Day and Time Criteria** без изменений.

- На вкладке **Log Source Criteria** установите флажок **Include the Selected Log Sources**, затем нажмите на кнопку **Add**.



Окно **Alarm Rule** window

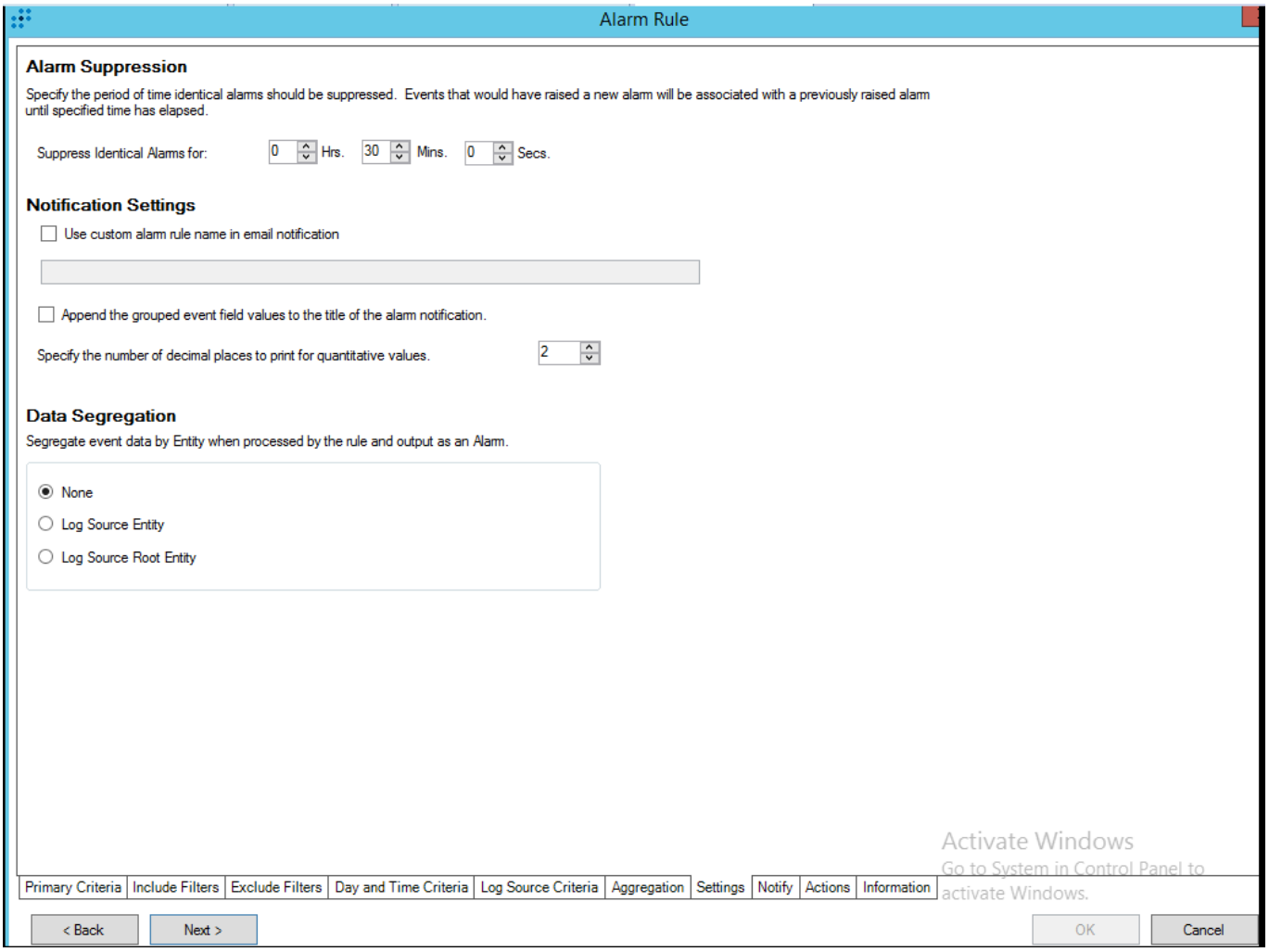
- Выберите источник, соответствующий Kaspersky CyberTrace, и нажмите на кнопку **OK**. Информацию о добавлении источника событий Kaspersky CyberTrace см. в разделе Добавление источника журналов в System Monitor Agent.



Окно **Log Source Criteria Add**

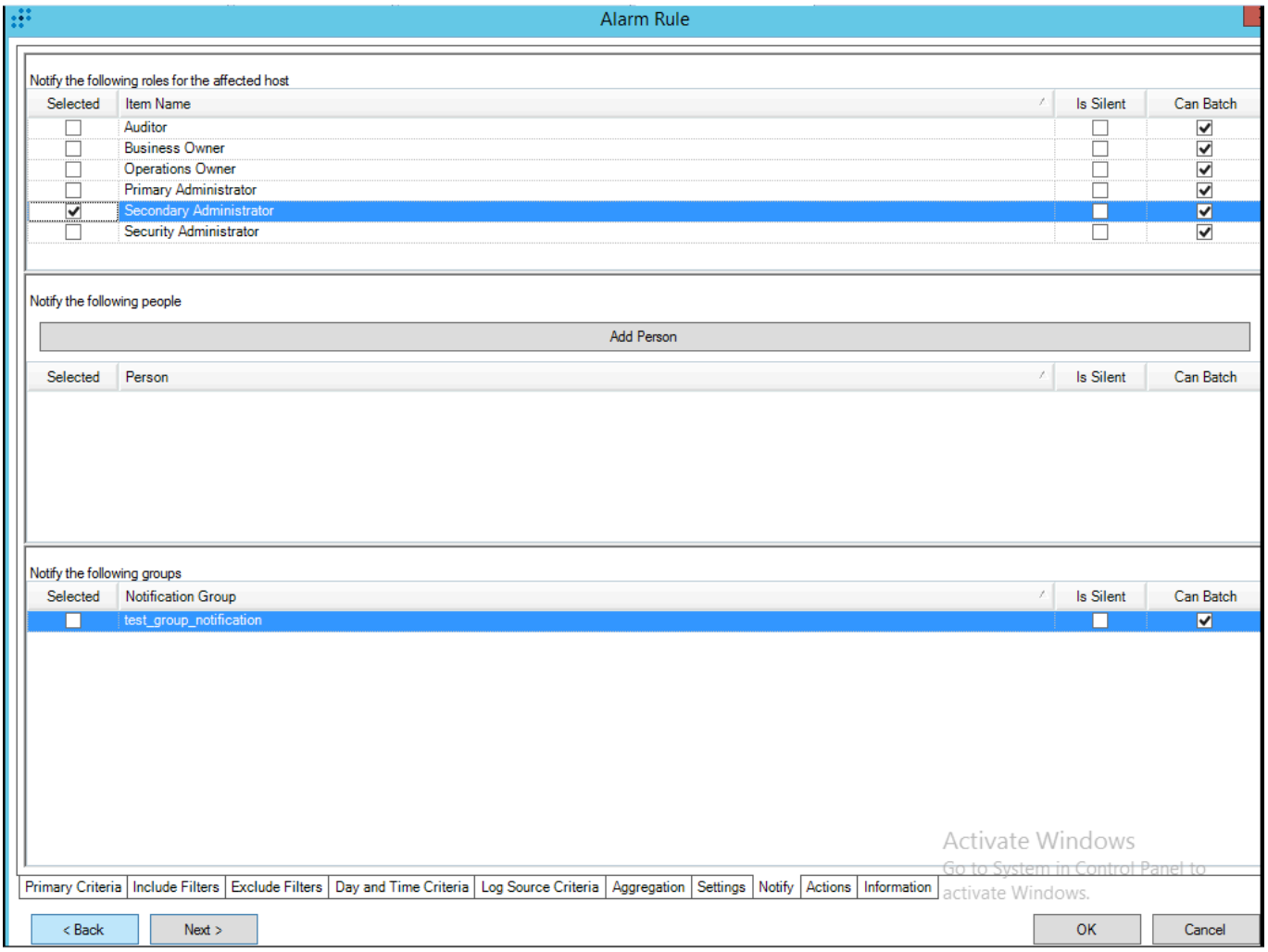
- Вкладку **Aggregation** оставьте без изменений.

- На вкладке **Settings** укажите период времени, в течение которого должны подавляться идентичные оповещения, связанные с возникновением каких-либо новых служебных событий Kaspersky CyberTrace.



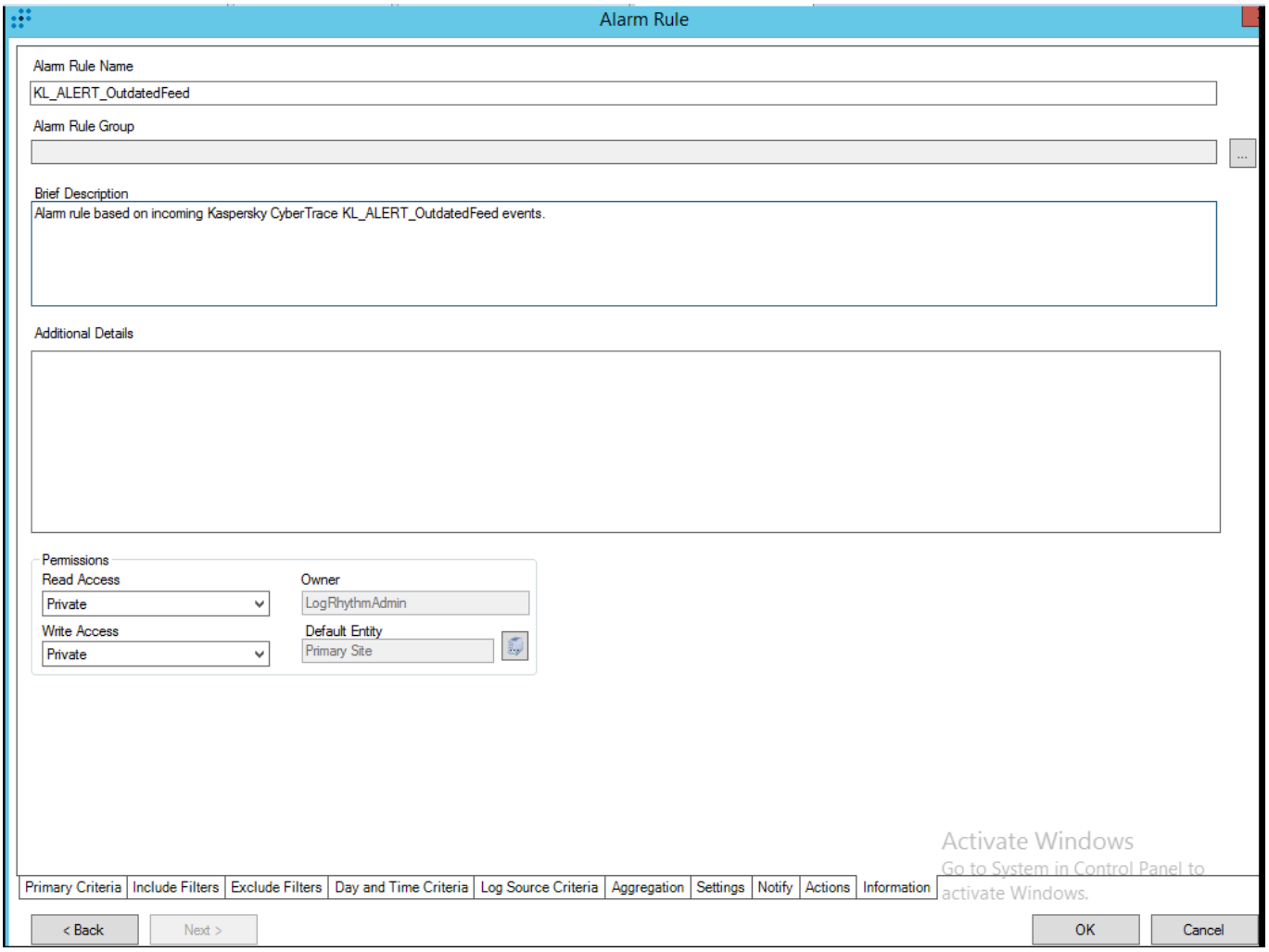
Параметры подавления оповещений

- На вкладке **Notify** выберите роль или пользователя, которым должны быть адресованы уведомления.



Выбор ролей для уведомления

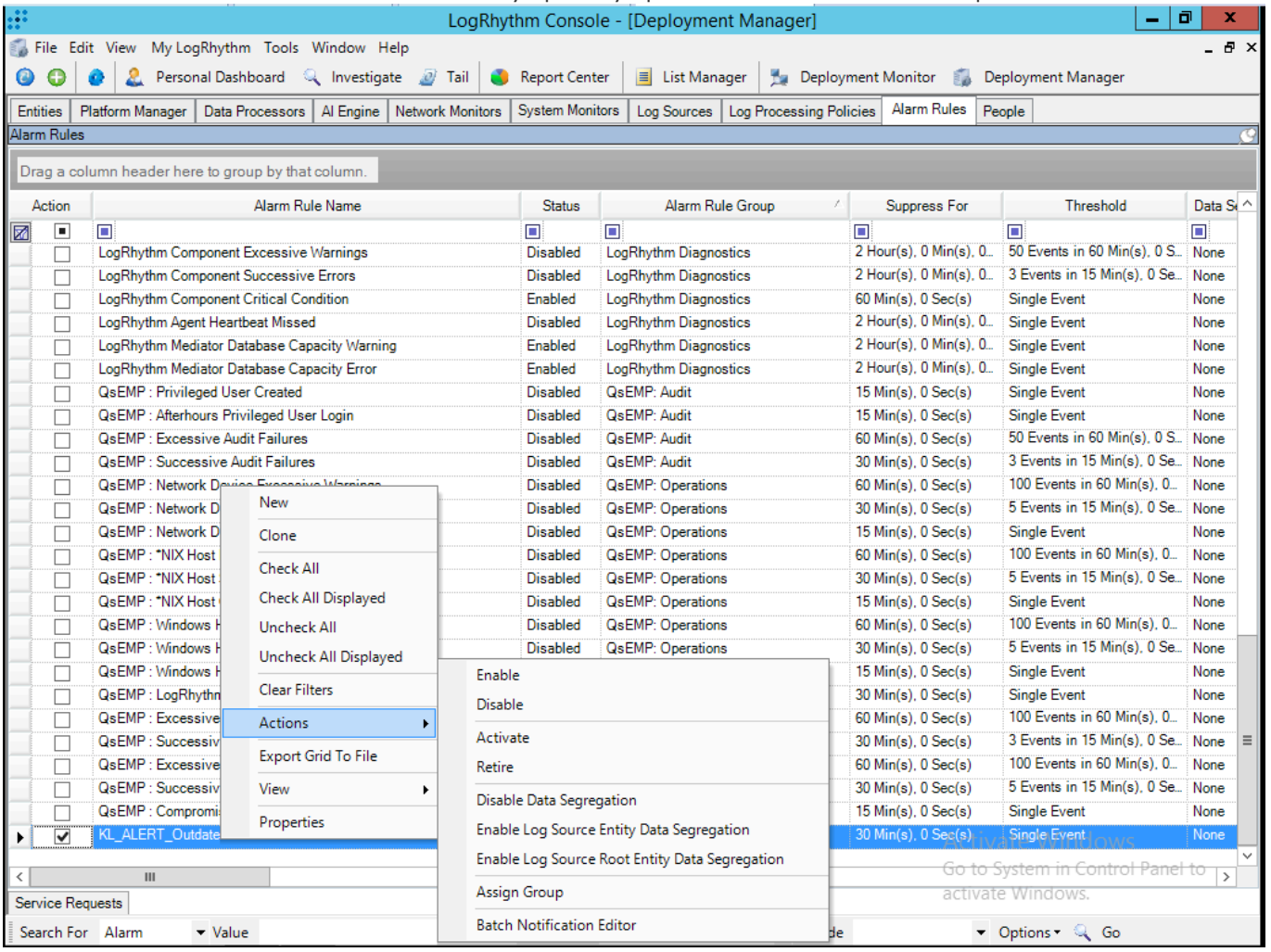
- Вкладку **Actions** оставьте без изменений.
- На вкладке **Information** укажите имя правила и его описание.



Alarm Rule Name/Brief Description

5. Нажмите на кнопку **OK**.

6. На вкладке **Alarm Rules** щелкните по новому правилу правой кнопкой мыши и выберите **Actions** → **Enable**.



Включение правила

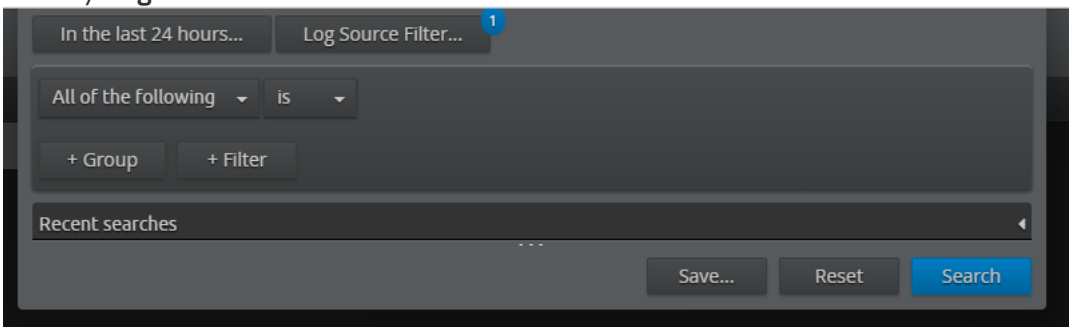
7. Настройте отображение оповещений в веб-консоли LogRhythm, как описано в разделе Шаг 10 (необязательный). Отображение оповещений о событиях в LogRhythm.

Шаг 10 (необязательный). Отображение служебных оповещений в LogRhythm

Веб-консоль LogRhythm можно настроить таким образом, чтобы служебные оповещения на ней отображались вместе с оповещениями об обнаружении индикаторов компрометации.

Чтобы настроить отображение оповещений о событиях в веб-консоли, выполните следующие действия:

1. В веб-консоли нажмите **Search**.
2. Нажмите на кнопку **Log Source Filter**.



Форма поиска

3. Введите `CyberTrace` в качестве строки поиска.
4. Переместите найденный фильтр поиска в правый столбец, для этого нажмите на стрелку (**+**).
5. Нажмите на кнопку **OK**.
6. После завершения нового поиска откройте окно результатов.

В веб-консоли LogRhythm в окне результатов поиска отображаются оповещения об обнаружении индикаторов компрометации вместе со служебными оповещениями.

Интеграция с McAfee Enterprise Security Manager

В этой главе описывается порядок интеграции Kaspersky CyberTrace с ПО для управления информацией и событиями в области безопасности (SIEM), таким как McAfee Enterprise Security Manager 11 (далее также «McAfee ESM»).

Приложение содержит сертификат для демоверсии Kaspersky Threat Data Feeds. При использовании демонстрационных потоков данных об угрозах обеспечивается более низкий уровень обнаружения по сравнению с соответствующими коммерческими версиями. Чтобы получить сертификат для коммерческой версии Kaspersky Threat Data Feeds, свяжитесь с командой Kaspersky CyberSecurity Service (intelligence@kaspersky.com).

Настройка Kaspersky CyberTrace для интеграции с McAfee Enterprise Security Manager

В этом разделе описывается порядок настройки Kaspersky CyberTrace для интеграции с McAfee ESM.

Чтобы настроить Kaspersky CyberTrace для интеграции с McAfee ESM, выполните следующие действия:

1. Загрузите Kaspersky CyberTrace со страницы https://support.kaspersky.com/datafeeds/download/15920.

2. Установка Kaspersky CyberTrace.

   - В ОС Linux Kaspersky CyberTrace устанавливается в каталог `/opt/kaspersky/ktfs`.

   - В случае установки в ОС Windows каталог установки в дальнейшем называется `%CyberTrace_installDir%`.

3. При первом входе в веб-интерфейс Kaspersky CyberTrace открывается *Мастер первоначальной настройки*. Следуйте инструкциям на экране. В частности, задайте следующие параметры:

   a. На шаге мастера **Настройка прокси-сервера** при необходимости укажите параметры подключения к прокси-серверу.

   b. На шаге мастера **Настройка управления данными** задайте параметры следующим образом:

      - В разделе **SIEM-система** выберите **Other**.

      - В блоке **Входящие события** укажите IP-адрес и порт, на котором Kaspersky CyberTrace будет прослушивать входящие события.

      - В блоке **Оповещения об обнаружении индикаторов компрометации** укажите IP-адрес и порт McAfee ESM, на который Kaspersky CyberTrace будет отправлять оповещения об обнаружении индикаторов компрометации обнаружения и служебные оповещения.

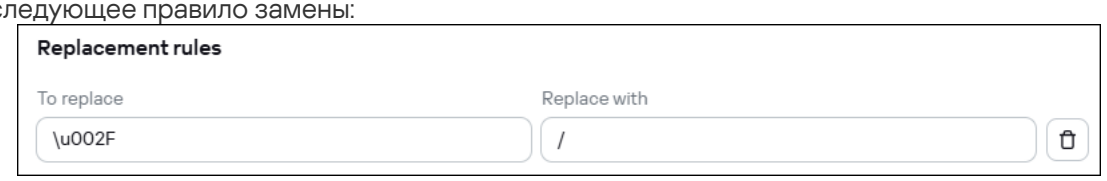
        В случае McAfee ESM это порт 514.

4. На странице **Параметры** → **Источники событий** нажмите кнопку (**Изменить**) рядом с источником событий **По умолчанию**, выберите вкладку **Регулярные выражения**, а затем укажите следующие регулярные выражения:

Регулярные выражения для интеграции с McAfee ESM

Тип индикатора	Название правила	Регулярное выражение	Дополнительные параметры
CONTEXT	Device	deviceExternalId\=(.*?)\s	
CONTEXT	DeviceAction	act\=(.*?)\s	
CONTEXT	DeviceIp	deviceTranslatedAddress\=(.*?)\s	
HASH	RE_HASH	([\da-fA-F]{32,64})	**Извлечь все**: True
IP	RE_IP	dst\=(.*?)\s	
Веб-адрес	RE_URL	(?:\:\/\/)((?:\S+(?::\S*)?+@)?(?:(?:(?:[a-z\x{00a1}-\x{ffff}0-9]+-*)*[a-z\x{00a1}-\x{ffff}0-9]*)(?:\.(?:[a-z\x{00a1}-\x{ffff}0-9]+-)*+[a-z\x{00a1}-\x{ffff}0-9]++)*(?:\.(?:[a-z\x{00a1}-\x{ffff}\-0-9]{2,}+)))(?:\.*:\d{2,5})?+(?:\.*\/[^\s\"\<\>]*+)?+)	**Извлечь все**: True
IP	SRC_IP	src\=(.*?)\s	
CONTEXT	UserName	duser\=(.*?)\s	

5. На вкладке **Правила нормализации** включите переключатель **Применять правила нормализации**, а затем укажите следующее правило замены:



Правило замены для интеграции с McAfee ESM

6. Сохраните изменения.

7. Выберите **Параметры** → **Служебные оповещения**, а затем укажите следующие форматы:

Формат служебных оповещений для интеграции с McAfee ESM

Поле	Значение
Формат служебных оповещений	`Событие службы Kaspersky CyberTrace | date=%Date% alert=%Alert% msg:%RecordContext%`
Формат контекста записей	`%ParamName%=%ParamValue%` Обратите внимание на пробел перед `%ParamName%`.

Сохраните изменения.

8. Выберите **Параметры** → **Оповещения об обнаружении индикаторов компрометации**, а затем укажите следующие форматы:

Формат оповещений об обнаружении индикаторов компрометации для интеграции с McAfee ESM

Поле	Значение
Формат → **Формат оповещения**	`Kaspersky CyberTrace Detection Event| date=%Date% reason=%Category% detected=%MatchedIndicator% act=%DeviceAction% dst=%RE_IP% src=%SRC_IP% hash=%RE_HASH% request=%RE_URL% dvc=%DeviceIp% sourceServiceName=%Device% suser=%UserName% msg:%RecordContext%`
Контекст → **Поля контекста**	`%ParamName%:%ParamValue%` Обратите внимание на пробел перед `%ParamName%`.

Сохраните изменения.

Пересылка событий из McAfee Enterprise Security Manager в Kaspersky CyberTrace

В этом разделе описывается, как пересылать события Kaspersky CyberTrace из McAfee Enterprise Security Manager в Kaspersky CyberTrace.

Чтобы настроить пересылку событий из McAfee Enterprise Security Manager в Kaspersky CyberTrace, выполните следующие действия:

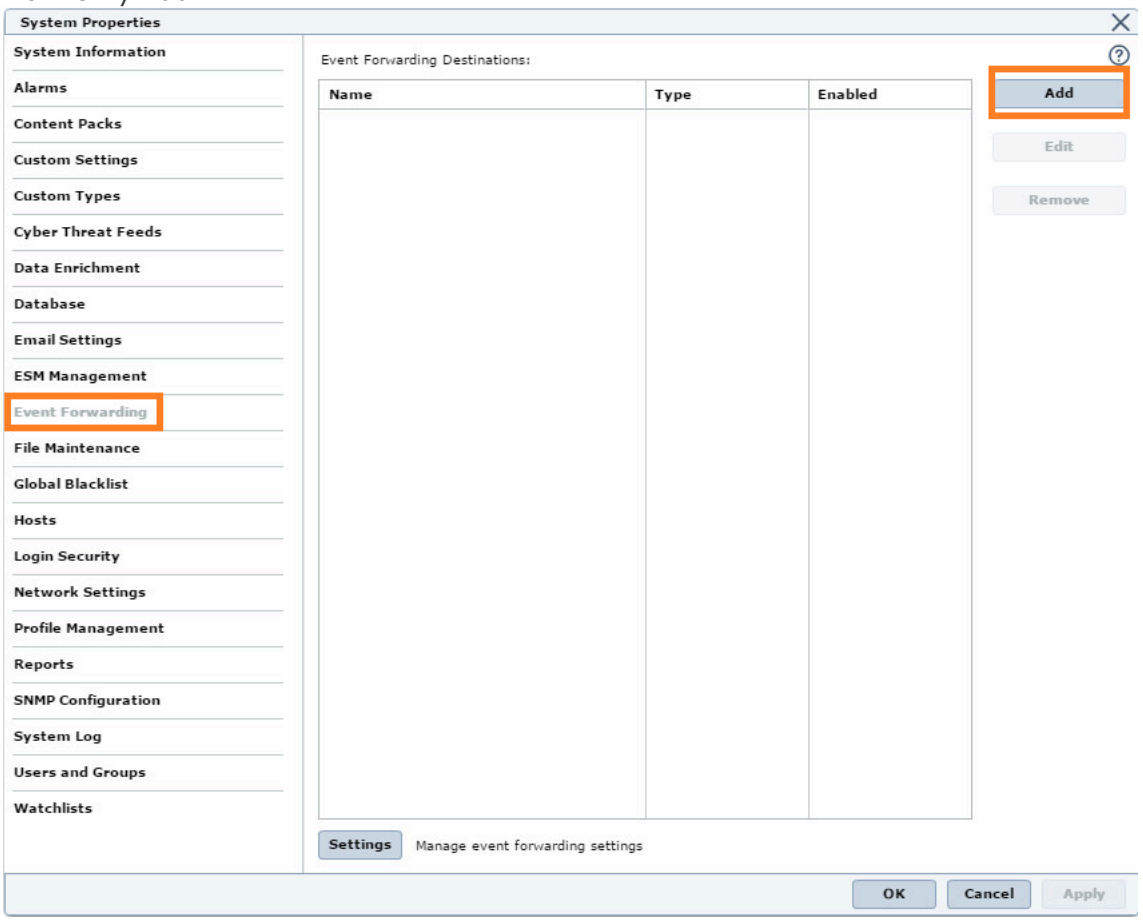
1. Откройте системные свойства McAfee ESM, нажав ≡ на информационной панели. В дереве навигации системы выберите **McAfee ESM** и нажмите кнопку **Properties**.

   Откроется диалоговое окно **System Properties**.

2. Нажмите **Event Forwarding**.

   Отобразятся параметры, относящиеся к пересылке событий.

3. Нажмите на кнопку **Add**.



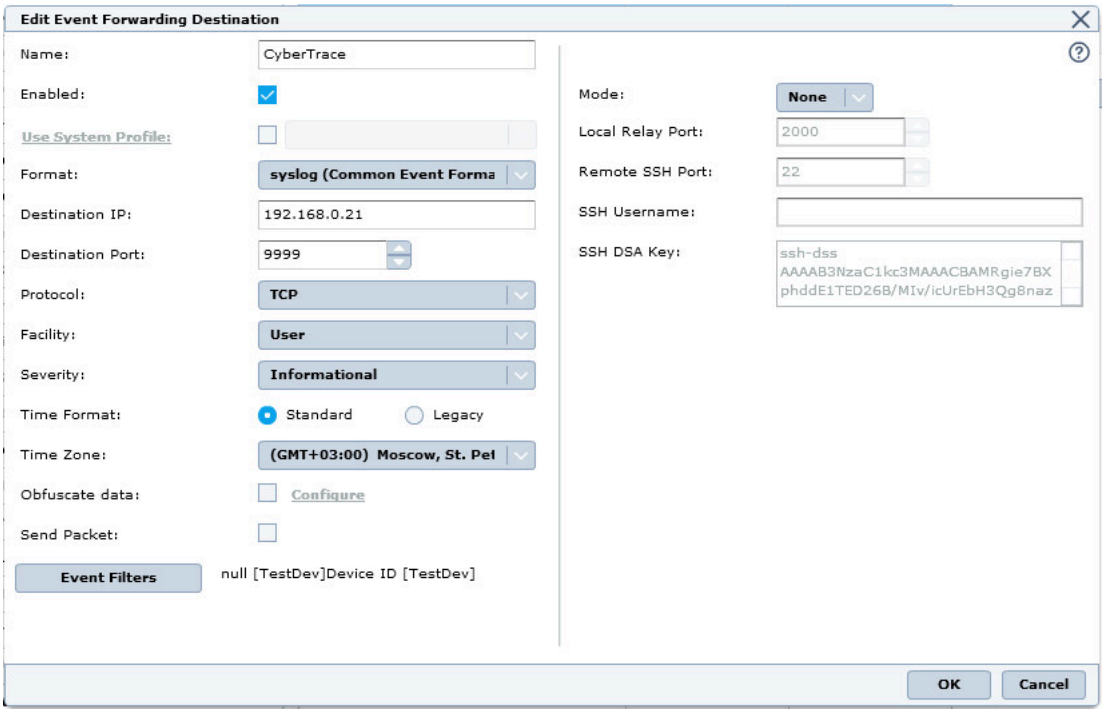
Диалоговое окно System Properties

4. В диалоговом окне **Edit Event Forwarding Destination** введите следующие данные:

   - **Name**: `CyberTrace`
   - **Enable**: `Selected`
   - **Use System Profile**: снят
   - **Format**: `Syslog (Common Event Format)`
   - **Destination IP**: IP-адрес сервера, на котором выполняется Kaspersky CyberTrace
   - **Destination Port**: порт, на котором Kaspersky CyberTrace прослушивает события

     IP-адрес и порт совпадают с указанными на вкладке **Параметры** → **Общие** веб-интерфейса Kaspersky CyberTrace.
   - **Protocol**: `TCP`
   - **Facility**: `User`
   - **Severity**: `Informational`
   - **Time Format**: `Standard`

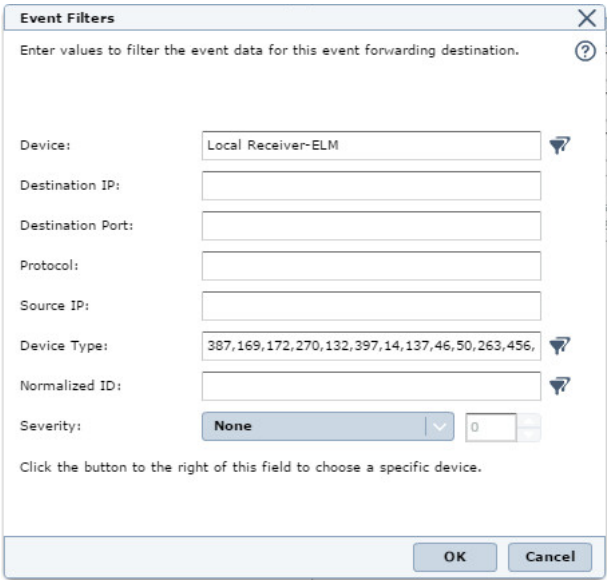
- **Time Zone**: выберите нужный часовой пояс
- **Obfuscate data**: снят
- **Send Packet**: снят
- **Mode**: None



Диалоговое окно Edit Event Forwarding Destination

5. Нажмите **Event Filters**.

   Откроется диалоговое окно **Event Filters**.

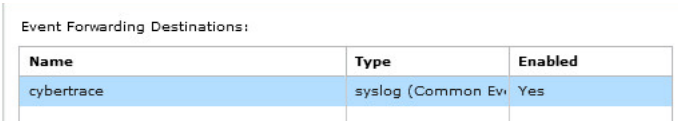


Диалоговое окно Event Filters

В диалоговом окне **Event Filters** можно указать источники событий, из которых события будут перенаправляться в Kaspersky CyberTrace. Например, можно указать следующие данные:

- Устройства, с которых пересылаются события
- Типы устройств, с которых пересылаются события

6. В диалоговом окне **Event Filters** нажмите кнопку **OK**.
7. В диалоговом окне **Edit Event Forwarding Destination** нажмите кнопку **OK**.
8. Убедитесь, что правило пересылки событий в Kaspersky CyberTrace отображается в McAfee Enterprise Security Manager.



Правило пересылки событий в Kaspersky CyberTrace

9. Убедитесь, что события поступают из McAfee Enterprise Security Manager. Если пересылка событий из McAfee Enterprise Security Manager в Kaspersky CyberTrace настроена правильно, на вкладке **Информационная панель** в веб-интерфейсе Kaspersky CyberTrace отобразится обновленная статистика индикаторов.

Парсинг служебных событий Kaspersky CyberTrace в McAfee Enterprise Security Manager

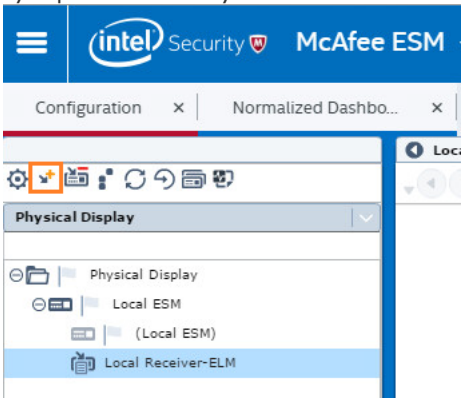
В этом разделе описывается порядок парсинга служебных событий Kaspersky CyberTrace, имеющих следующий формат:

```
Kaspersky CyberTrace Service Event| date=%Date% alert=%Alert% msg:%RecordContext%
```

Обратите внимание, что при изменении формата служебных событий необходимо изменить правила обработки служебных событий в McAfee Enterprise Security Manager.

*Для парсинга события службы введите следующие данные в диалоговом окне **Advanced Syslog Parser Rule**:*

1. В главном окне McAfee Enterprise Security Manager нажмите **Configuration**.
2. В дереве **Physical Display** выберите устройство-получатель и нажмите **Add Data Source**.



Добавление источника данных

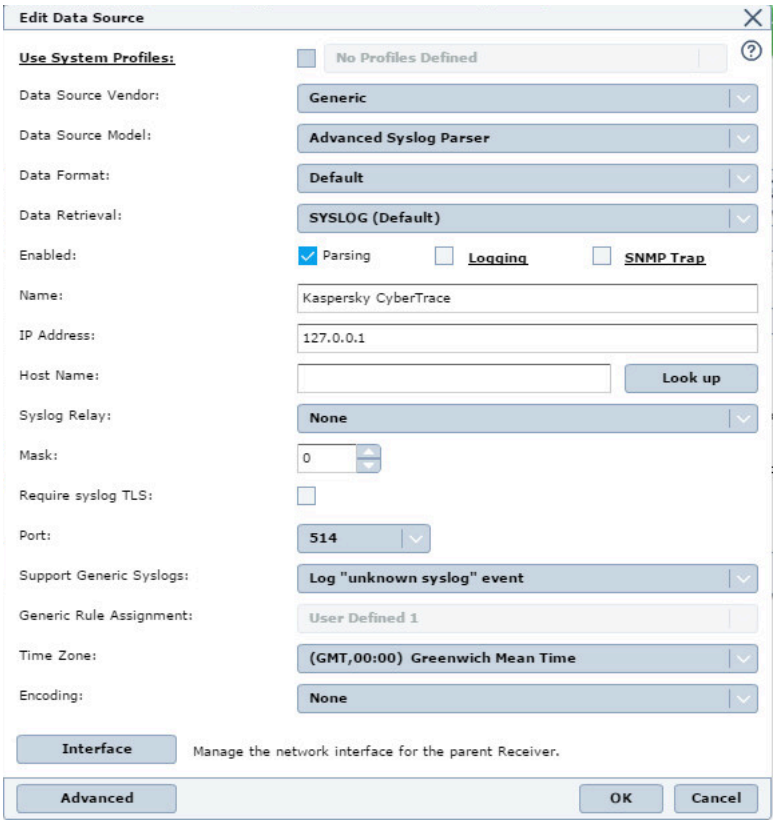
Откроется диалоговое окно **Add Data Source**.

3. В диалоговом окне **Add Data Source** введите следующие данные:

   - **Data Source Vendor**: Generic
   - **Data Source Model**: Advanced Syslog Parser
   - **Data Format**: Default
   - **Data Retrieval**: SYSLOG (по умолчанию)
   - **Enabled**: Parsing
   - **Name**: Kaspersky CyberTrace
   - **IP**: IP-адрес сервера, с которого Kaspersky CyberTrace будет отправлять события.
   - **Syslog Relay**: None
   - **Mask**: 0
   - **Require syslog TLS**: Cleared
   - **Port**: 514
   - **Support Generic Syslogs**: Log "unknown syslog" event

     McAfee Enterprise Security Manager получает все события из Kaspersky CyberTrace. Если McAfee Enterprise Security Manager не может выполнить парсинг события, оно отображается как неизвестное.

- **Time Zone**: выберите нужный часовой пояс
- **Encoding**: None

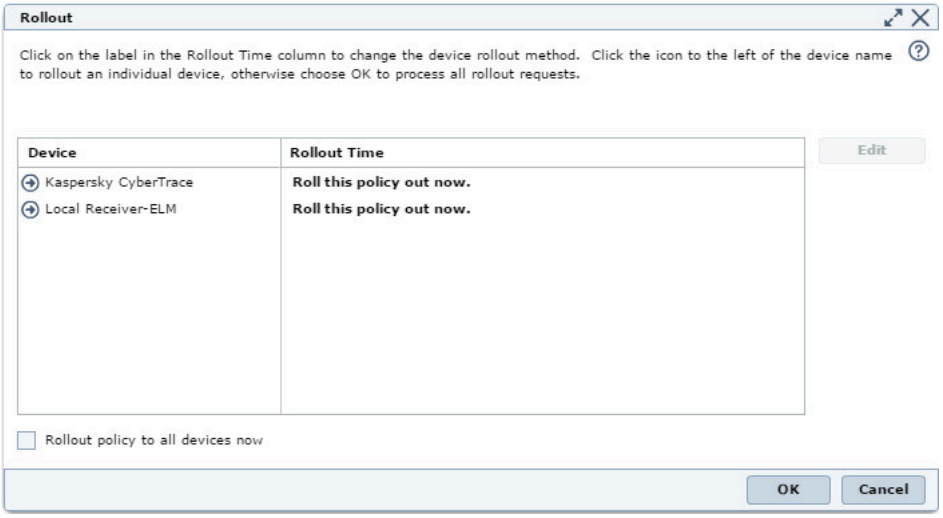


Конфигурация источника данных

4. (Необязательно) Нажмите **Advanced**, чтобы указать параметры источника данных в диалоговом окне **Advanced options**.

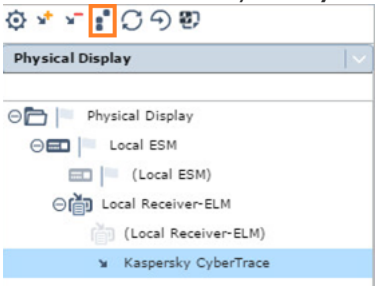
5. Нажмите на кнопку **OK**.

   McAfee ESM предлагает развернуть настроенную политику.



Диалоговое окно Rollout

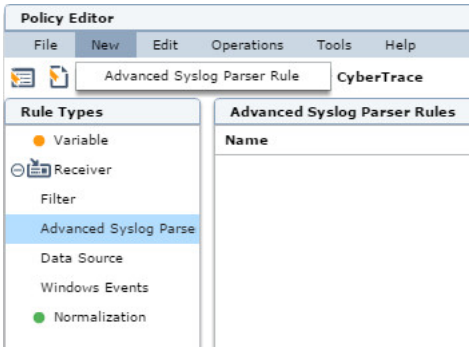
6. Выберите **Kaspersky CyberTrace**, а затем нажмите кнопку **Policy Editor** на панели инструментов.



Выбор в Policy Editor

7. В окне **Policy Editor** выберите тип правил **Advanced Syslog Parser Rules**.

8. Нажмите **New** → **Advanced Syslog Parser Rule**.



Окно Policy Editor

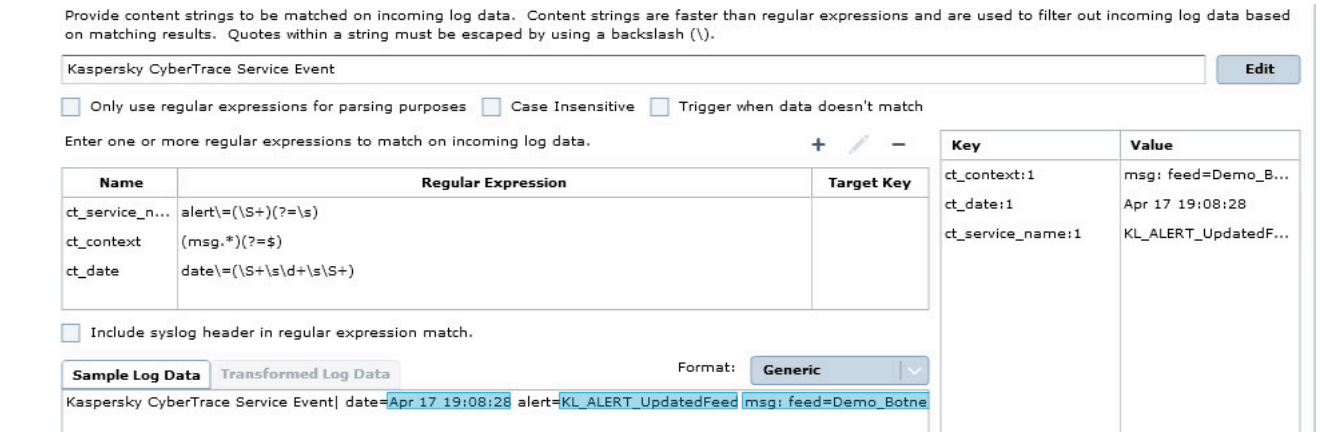
9. Чтобы создать парсер для анализа событий обновления потока данных, введите следующие данные в диалоговом окне **Advanced Syslog Parser Rule**:

   - На вкладке **General** введите следующие данные:
     - **Name**: `Kaspersky_CyberTrace_ServiceEvent`
     - **Tags**: выберите теги, определяющие правило (они будут использоваться при фильтрации событий)
     - **Rule Assignment Type**: User Defined 1 или другой определяемый пользователем тип
     - **Description**: событие службы Kaspersky CyberTrace
   - На вкладке **Parsing** введите следующие данные:
     - **Provide content strings**: событие службы Kaspersky CyberTrace
     - **Sample Log Data**: предоставьте пример события обновления потока данных. Например (в одну строку, без символов новой строки):

       ```
       Kaspersky CyberTrace Service Event| date=Apr 17 19:08:28
       alert=KL_ALERT_UpdatedFeed msg:feed=Demo_Botnet_CnC_URL_Data_Feed.json
       records=3907
       ```

     - Добавьте следующие регулярные выражения на вкладке **Parsing**:

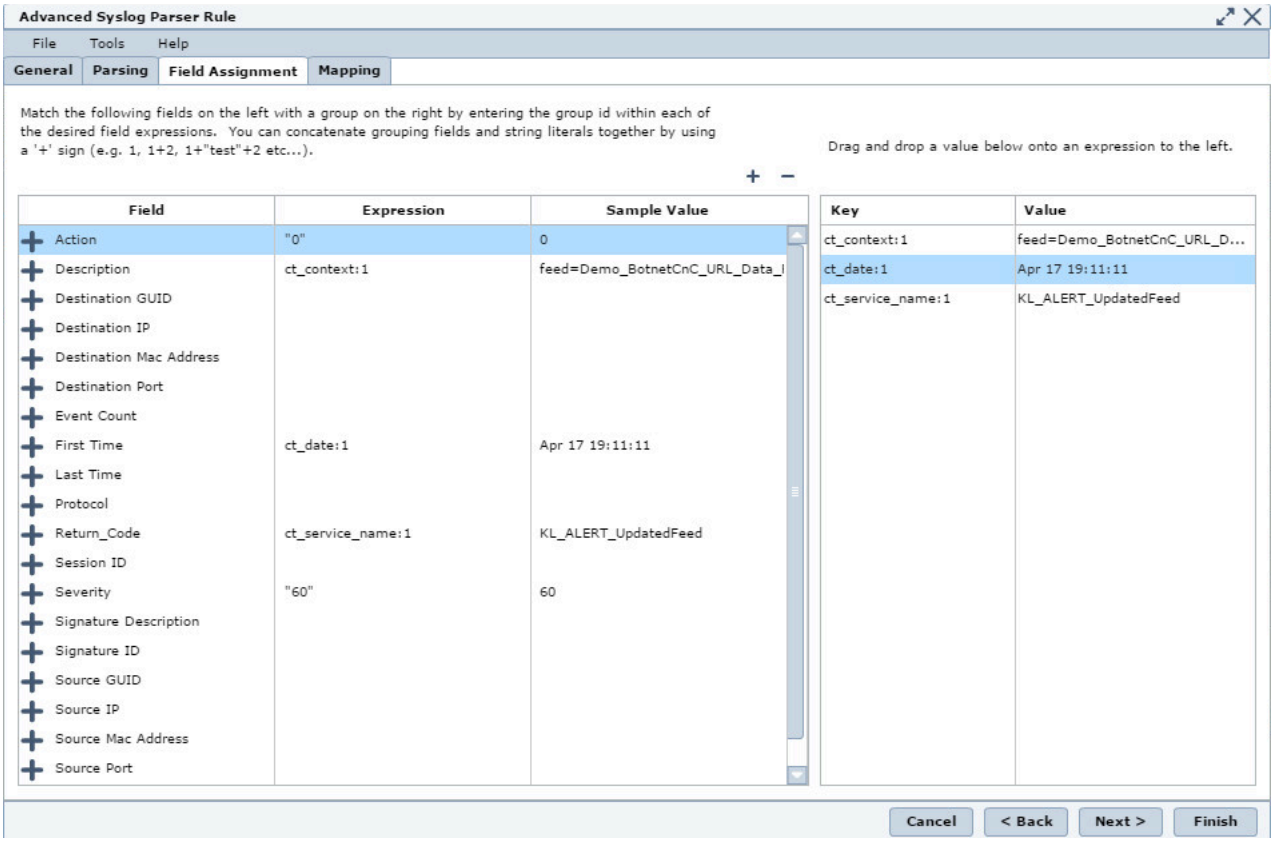
Название	Регулярное выражение
ct_service_name	alert\=(\S+)(?=\s)
ct_context	(msg.*)(?=$)
ct_date	date\=(\S+\s\d+\s\S+)



Вкладка Parsing

- На вкладке **Field Assignment** введите следующие данные:

Поле	Выражение
Action	"0"
Описание	Перетащите ct_context в это поле
Severity	"60" или другое значение по вашему выбору
Return_Code	Перетащите ct_service_name в это поле
First Time	Перетащите ct_date в это поле



Вкладка Field Assignment

Вы можете добавить другие поля, нажав на кнопку **+**.

- На вкладке **Mapping** введите следующие данные:
  - В таблице временных данных:

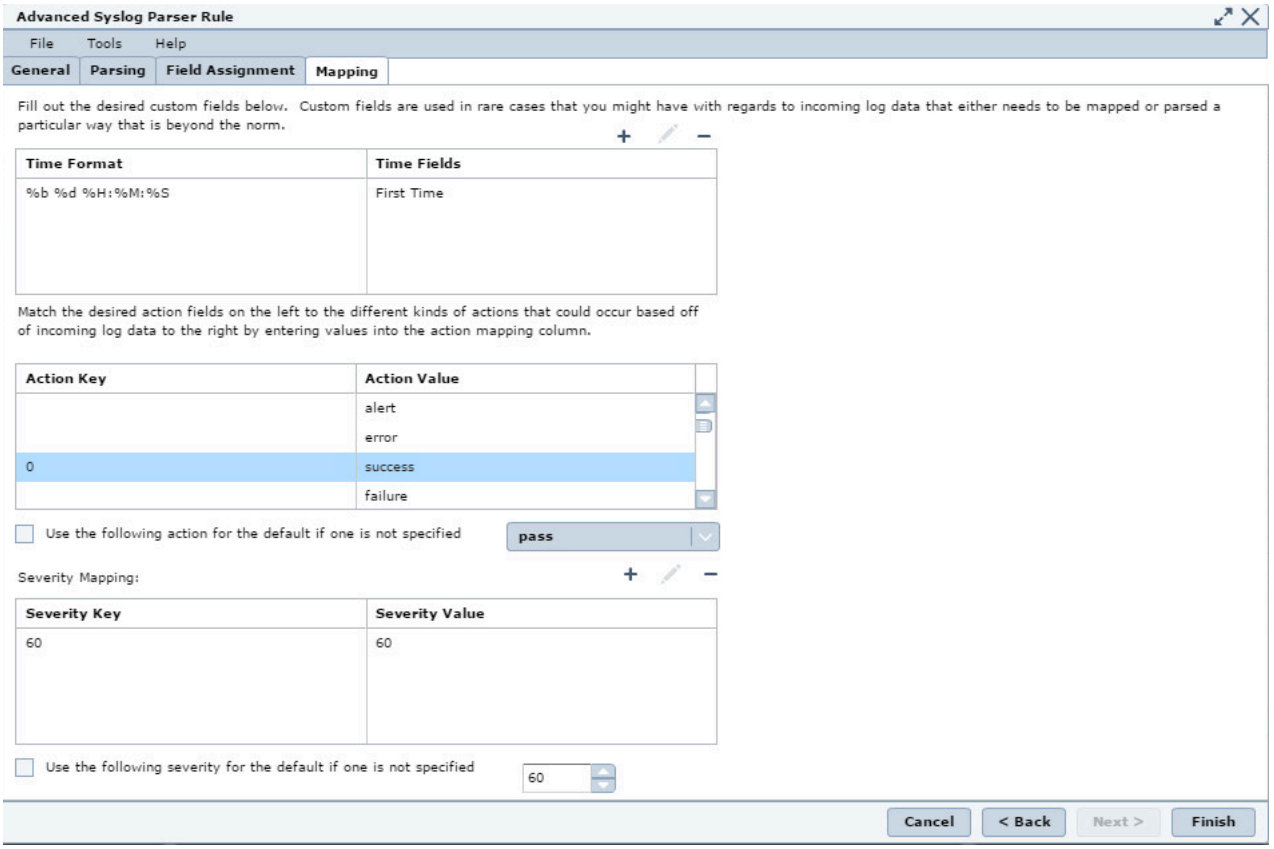
Формат времени	Поля времени
`%b %d %H:%M:%S`	`First time`

- В таблице действий:

Ключ действия	Значение действия
`0`	`Success`

- В таблице важности:

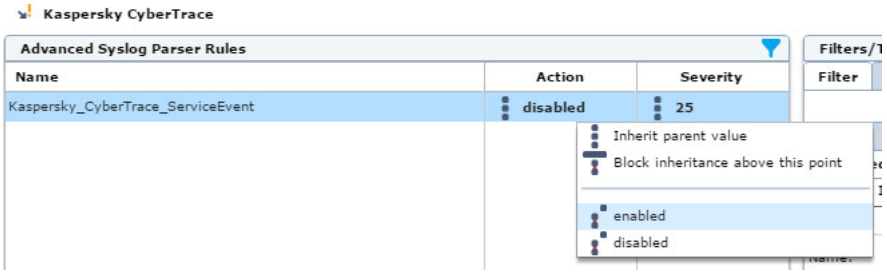
Ключ важности	Значение важности
`60`	`60`



Вкладка Mapping

10. Нажмите на кнопку **Finish**, чтобы сохранить политику.

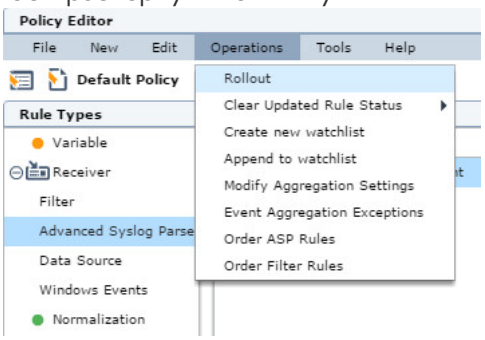
11. В списке **Default Policy** выберите устройство `Kaspersky CyberTrace`, а затем включите правило `Kaspersky_CyberTrace_ServiceEvent`.



Включение правила

12. Выберите **File** → **Save**, чтобы сохранить текущее состояние.

13. Выберите **Operations** → **Rollout**, чтобы развернуть политику.

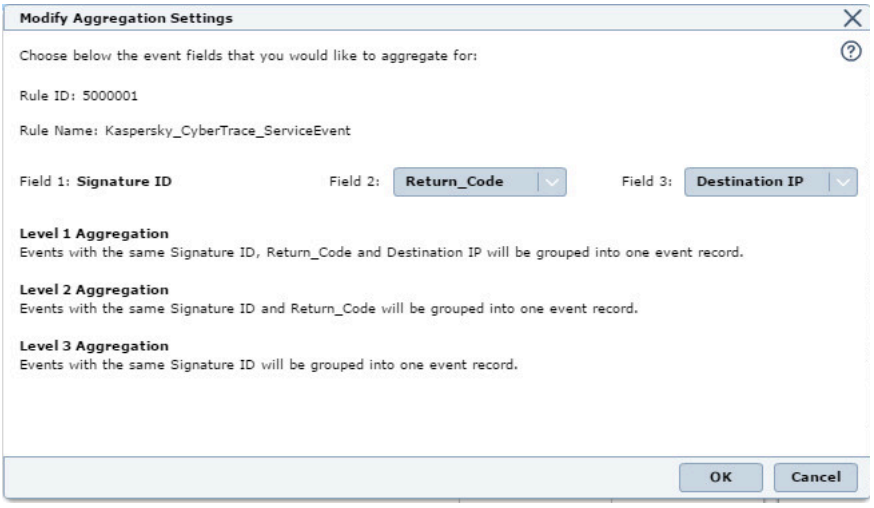


Развертывание политики

14. При появлении запроса согласитесь на повторную инициализацию устройства `Kaspersky CyberTrace` в McAfee ESM.

15. Выберите пункт меню **Operations** → **Modify Aggregation Settings**, чтобы изменить правила агрегирования служебных событий Kaspersky CyberTrace.

16. В окне **Modify Aggregation Settings** в поле `Field 2` задайте значение `Return_Code` и нажмите кнопку **OK**.



Modify Aggregation Settings

17. Подтвердите запрос на развертывание.

Парсинг событий обнаружения Kaspersky CyberTrace в McAfee Enterprise Security Manager

В этом разделе описывается порядок парсинга событий обнаружения киберугроз Kaspersky CyberTrace, имеющих следующий формат:

```
Kaspersky CyberTrace Detection Event| date=%Date% reason=%Category%
detected=%MatchedIndicator% act=%DeviceAction% dst=%RE_IP% src=%SRC_IP% hash=%RE_HASH%
request=%RE_URL% dvc=%DeviceIp% sourceServiceName=%Device% suser=%UserName%
msg:%RecordContext%
```

Обратите внимание, что в случае изменения формата событий обнаружения киберугроз Kaspersky CyberTrace необходимо изменить правила парсера Kaspersky CyberTrace в McAfee ESM.

*Для парсинга события обнаружения введите следующие данные в диалоговом окне **Advanced Syslog Parser Rule**:*

- На вкладке **General** введите следующие данные:
  - **Name**: `Kaspersky_CyberTrace_DetectionEvent`
  - **Tags**: выберите теги, определяющие правило (они будут использоваться при фильтрации событий)
  - **Rule Assignment Type**: User Defined 1
  - **Description**: событие обнаружения Kaspersky CyberTrace
- На вкладке **Parsing** введите следующие данные:
  - **Provide content strings**: событие обнаружения Kaspersky CyberTrace
  - **Sample Log Data**: приведите пример события обнаружения URL. Например:

    ```
    Kaspersky CyberTrace Detection Event| date=Oct 12 16:13:23 reason=KL_BotnetCnC_URL
    detected=http://fakess123bn.nu act=REQUEST_URL dst=192.168.1.0 src=192.168.2.0
    hash=776735A8CA96DB15B422879DA599F474 request=http://fakess123bn.nu dvc=192.168.3.0
    sourceServiceName=FireWall suser=UserName msg:popularity=5 geo=vn, in, mx
    threat=Trojan.Win32.Waldek
    ```

  - Добавьте следующие регулярные выражения для парсинга событий:

Название	Регулярное выражение
ct_date	date\=(\S+\s\d+\s\S+)
ct_reason	reason\=(.*)\sdetected
ct_indicator	detected\=(.*)\sact
ct_dev_action	act\=(.*)\sdst
ct_dst	dst\=(\S+)
ct_src	src\=(\S+)
ct_hash	hash\=(\S+)

Название	Регулярное выражение
ct_request	request\=(.*)\sdvc
ct_dev_ip	dvc\=(\S+)
ct_serviceName	sourceServiceName\=(.*)\ssuser
ct_username	suser\=(.*?)\smsg
ct_context	msg\:(.*)$

- На вкладке **Field Assignment** введите следующие данные:

Поле	Выражение
Action	"0"
First Time	Перетащите ct_date в это поле
Веб-адрес	Перетащите ct_request в это поле
Destination IP	Перетащите ct_dst в это поле
Device_Action	Перетащите ct_dev_action в это поле
Хеш	Перетащите ct_hash в это поле
Хост	Перетащите ct_dev_ip в это поле
Message_Text	Перетащите ct_context в это поле
Object	Перетащите ct_indicator в это поле
Return_Code	Перетащите ct_reason в это поле
Service_Name	Перетащите ct_serviceName в это поле
Severity	"80"
Source IP	Перетащите ct_src в это поле
Source User	Перетащите ct_username в это поле

McAfee ESM переименовывает поле `Object` в `ObjectID`.

- На вкладке **Mapping** введите следующие данные:
  - В таблице временных данных укажите следующие данные:

Формат времени	Поля времени
%b %d %H:%M:%S	First time

- В таблице действий укажите следующие данные:

Ключ действия	Значение действия
0	Success

- В таблице важности укажите следующие данные:

Ключ важности	Значение важности
80	80

После указания вышеприведенных значений выполните следующие действия:

1. В списке **Default Policy** выберите устройство `Kaspersky CyberTrace`, а затем включите правило `Kaspersky_CyberTrace_DetectionEvent`.
2. Выберите **File** → **Save**, чтобы сохранить текущее состояние.
3. Выберите **Operations** > **Rollout**, чтобы развернуть политику.
4. Повторно инициализируйте устройство `Kaspersky CyberTrace`.
5. Выберите **Operations** → **Modify Aggregation Settings**, чтобы изменить правила агрегирования служебных событий Kaspersky CyberTrace.

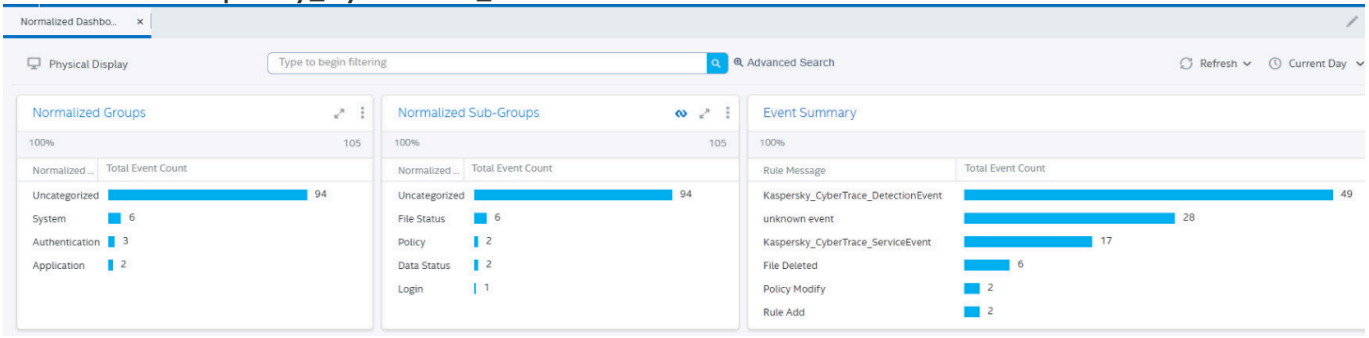
   Откроется диалоговое окно **Modify Aggregation Settings**.
6. Укажите следующие значения:
   - Установите для параметра `Field 2` значение `Object`.
   - Установите для параметра `Field 3` значение `Return_Code`.
7. Нажмите на кнопку **OK**.
8. Подтвердите запрос на развертывание.

Просмотр событий Kaspersky CyberTrace в McAfee Enterprise Security Manager

В этом разделе описан порядок просмотра событий Kaspersky CyberTrace в McAfee ESM.

Чтобы просмотреть события из Kaspersky CyberTrace:

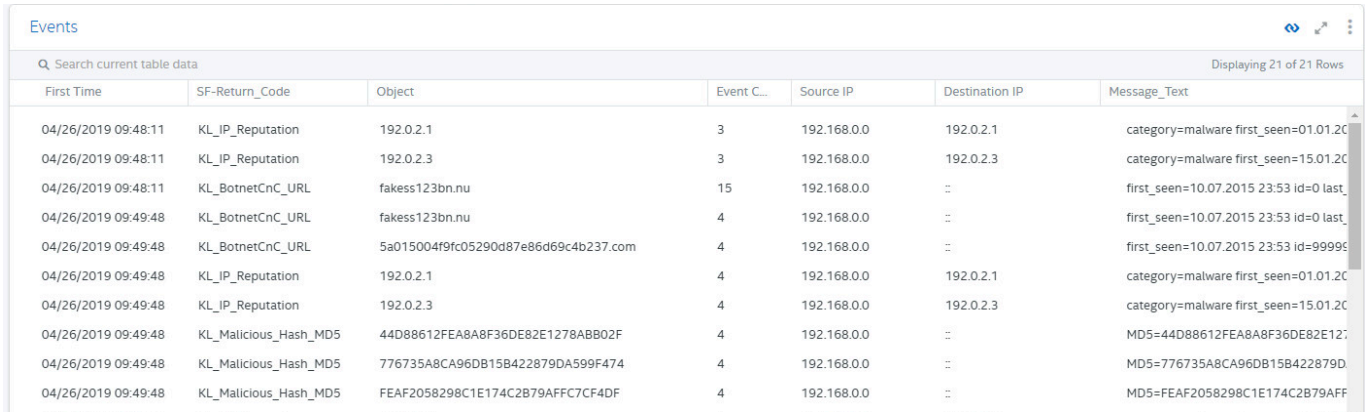
1. Выберите вкладку **Normalized Dashboard** и в таблице **Event Summary** найдите строки, текст в которых начинается с **Kaspersky_CyberTrace_**.



Просмотр сводки событий

2. Выберите строку в таблице **Event Summary**.

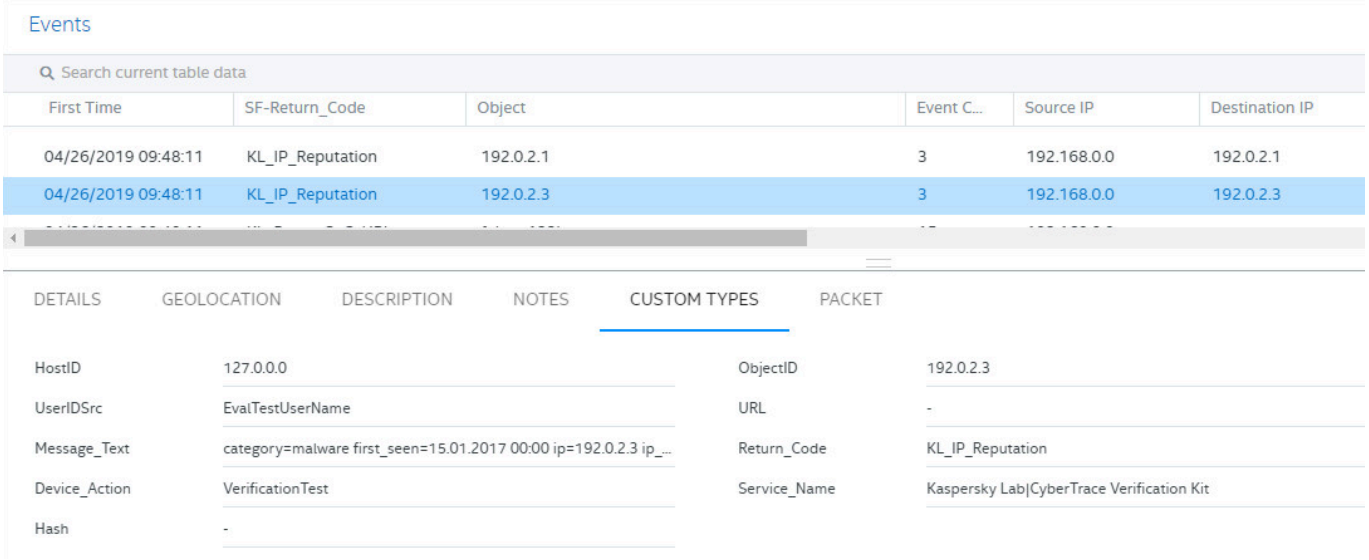
Таблица **Events** будет содержать события из Kaspersky CyberTrace.



Список событий Kaspersky CyberTrace

3. Выберите строку в таблице **Events**.

   Полная информация о выбранном событии будет показана под таблицей **Events**.



Просмотр информации о событии

Инструкции по созданию оповещений и предупреждений см. в документации по McAfee ESM.

Интеграция с AlienVault USM / OSSIM

В этой главе описывается, как интегрировать потоки данных об угрозах Kaspersky Threat Data Feeds с AlienVault USM (или AlienVault OSSIM).

Мы рекомендуем интегрировать потоки данных об угрозах Kaspersky Threat Data Feeds с AlienVault USM / OSSIM с помощью Kaspersky CyberTrace.

Шаги интеграции с AlienVault USM / OSSIM

Для интеграции потоков данных "Лаборатории Касперского" об угрозах с AlienVault USM / OSSIM необходимо выполнить следующие действия:

1. Настройка Kaspersky CyberTrace для интеграции с AlienVault USM / OSSIM.
2. Настройка AlienVault USM / OSSIM для пересылки событий в Kaspersky CyberTrace.
3. Добавление источника событий Kaspersky CyberTrace в AlienVault USM / OSSIM.

После интеграции события Kaspersky CyberTrace можно будет просматривать в AlienVault USM / OSSIM.

Настройка Kaspersky CyberTrace для интеграции с AlienVault USM / OSSIM

В этом разделе описывается порядок настройки Kaspersky CyberTrace для интеграции с AlienVault USM / OSSIM.

Kaspersky CyberTrace и устройство, события которого будут пересылаться в Kaspersky CyberTrace, должны работать на разных серверах. Правила пересылки основаны на IP-адресах. Следовательно, IP-адрес сервера, на котором установлена программа Kaspersky CyberTrace, должен отличаться от IP-адресов устройств, события которых необходимо пересылать в Kaspersky CyberTrace.

Для настройки интеграции с AlienVault USM / OSSIM в Kaspersky CyberTrace необходимо выполнить следующие действия:

1. Загрузите Kaspersky CyberTrace со страницы https://support.kaspersky.com/datafeeds/download/15920.
2. Установка Kaspersky CyberTrace.
   - В ОС Linux Kaspersky CyberTrace устанавливается в каталог `/opt/kaspersky/ktfs`.
   - В случае установки в ОС Windows каталог установки в дальнейшем называется `%CyberTrace_installDir%`.
3. При первом входе в веб-интерфейс Kaspersky CyberTrace открывается *Мастер первоначальной настройки*.

   Укажите следующие параметры Kaspersky CyberTrace:

   - IP-адрес сервера, на котором выполняется AlienVault USM / OSSIM, и порт `514`.

     Это IP-адрес и порт, на которые Kaspersky CyberTrace отправляет события обнаружения.

   - IP-адрес сервера, на котором выполняется Kaspersky CyberTrace, и любой доступный порт (например, `9999`).

     Это IP-адрес и порт, на которые AlienVault USM / OSSIM отправляет события для проверки. Это порт, на котором Kaspersky CyberTrace прослушивает входящие события.

   - Следующий формат служебного события:

     ```
     alert=%Alert% context=%RecordContext%
     ```

- Следующий формат события обнаружения киберугрозы:

  `category=%Category% detected=%MatchedIndicator% url=%RE_URL% src=%SRC_IP% ip=%RE_IP% hash=%RE_MD5% context=%RecordContext%`

4. В файле kl_feed_service.conf установите для атрибута `enabled` элемента `OutputSettings > FinishedEventFormat` значение `false`.

5. Сохраните файл kl_feed_service.conf.

6. Перезапустите Kaspersky CyberTrace с помощью веб-интерфейса Kaspersky CyberTrace или скрипта kl_feed_service.

Пересылка событий из AlienVault USM / OSSIM в Kaspersky CyberTrace

Чтобы настроить пересылку событий в Kaspersky CyberTrace на стороне AlienVault USM / OSSIM, выполните следующие действия:

Чтобы настроить AlienVault USM / OSSIM для пересылки событий в Kaspersky CyberTrace, выполните следующие действия:

1. Для каждого устройства, с которого события будут перенаправляться в Kaspersky CyberTrace, добавьте следующее правило в файл `/etc/rsyslog.conf`:

   ```
   if ($fromhost-ip == '%DEVICE_IP%') then {action (type="omfwd"
   Target="%CyberTrace_IP_IN%" Port="%CyberTrace_PORT_IN%" Protocol="tcp"
   Device="%INTERFACE%") action (type="omfile" File="%PATH%")}
   ```

   Параметры здесь имеют следующий смысл:

   - `%CyberTrace_IP_IN%` – IP-адрес сервера, на котором выполняется Kaspersky CyberTrace.
   - `%CyberTrace_PORT_IN%` — порт, который Kaspersky CyberTrace прослушивает для получения событий.
   - `%INTERFACE%` – имя сетевого интерфейса сервера, на котором выполняется AlienVault USM / OSSIM, который будет использоваться для пересылки событий в Kaspersky CyberTrace.

     Например, `eth0`.

   - `%DEVICE_IP%` – IP-адрес устройства, события с которого поступают в AlienVault USM / OSSIM и должны быть пересланы в Kaspersky CyberTrace.
   - `action (type="omfile" File="%PATH%")` – инструкции для службы rsyslog по сохранению в AlienVault USM / OSSIM событий, которые пересылаются в Kaspersky CyberTrace.

     `%PATH%` – путь к файлу, в котором будут храниться события. `%PATH%` может быть любым файлом, в котором вы хотите хранить пересылаемые события.

     `action (type="omfile" File="%PATH%")` – необязательно. Вы можете указать эту команду в процессе интеграции, чтобы проверить следующее:

     - тот факт, что события пересылаются в Kaspersky CyberTrace;
     - список событий, перенаправляемых в Kaspersky CyberTrace.

     По завершении процесса интеграции рекомендуется удалить эту строку из файла конфигурации.

   Это правило необходимо добавить после текста `# rsyslog zasec.conf`. Если этого текста нет в файле конфигурации, добавьте правило перед следующими строками:

```
if not ($fromhost-ip == '127.0.0.1') then -/var/log/ossim/asec_unk.log
if not ($fromhost-ip == '127.0.0.1') then ~
```

2. Перезапустите службу rsyslog следующей командой:

```
/etc/init.d/rsyslog restart
```

Импорт файлов конфигурации в AlienVault USM / OSSIM

В этом разделе описывается, как настроить AlienVault USM / OSSIM для обработки Kaspersky CyberTrace как источника событий. Чтобы настроить AlienVault USM / OSSIM соответствующим образом, необходимо на компьютере с AlienVault USM / OSSIM выполнить действия в следующем порядке:

Чтобы настроить получение событий из Kaspersky CyberTrace в AlienVault USM / OSSIM, выполните следующие действия:

1. Скопируйте следующие конфигурационные файлы в их целевые каталоги:

   - Скопируйте файл kaspersky_cyberTrace.cfg в каталог `/etc/ossim/agent/plugins/`.
   - Скопируйте файл kaspersky_cyberTrace.sql в каталог `/usr/share/doc/ossim-mysql/contrib/plugins/`.

   Файлы kaspersky_cyberTrace.cfg и kaspersky_cyberTrace.sql поставляются вместе с данной справочной документацией или предоставляются менеджером по работе с клиентами.

2. Добавьте следующую строку в раздел `plugins` файла `/etc/ossim/agent/config.cfg`:

   ```
   kaspersky_cyberTrace =/etc/ossim/agent/plugins/kaspersky_cyberTrace.cfg
   ```

3. Добавьте следующее правило в файл `/etc/rsyslog.conf`:

   ```
   if ($fromhost-ip == '%CyberTrace_IP_OUT%') then -/var/log/kaspersky_cyberTrace.log
   ```

   Здесь `%CyberTrace_IP_OUT%` – IP-адрес сервера, с которого Kaspersky CyberTrace отправляет события.

   Рекомендуется добавлять эту строку перед правилами, которые добавляются при настройке AlienVault USM / OSSIM для пересылки событий в Kaspersky CyberTrace.

4. Выполните следующую команду:

   ```
   cat /usr/share/doc/ossim-mysql/contrib/plugins/kaspersky_cyberTrace.sql | ossim-db
   ```

   Эта команда добавляет информацию о Kaspersky CyberTrace в базу данных AlienVault.

5. Выполните следующую команду:

   ```
   /etc/init.d/ossim-agent restart
   /etc/init.d/ossim-server restart
   ```

   С помощью этой команды AlienVault USM / OSSIM применяет настройки, заданные в файле конфигурации kaspersky_cyberTrace.cfg. Этот файл содержит правила, которые AlienVault USM / OSSIM использует для парсинга событий Kaspersky CyberTrace.

6. Перезапустите службу rsyslog следующей командой:

   ```
   /etc/init.d/rsyslog restart
   ```

7. Настройте утилиту `logrotate` для архивирования событий Kaspersky CyberTrace на сервере, на котором работает AlienVault USM / OSSIM.

   a. Создайте файл `kaspersky_cybertrace` в каталоге `/etc/logrotate.d`.

   b. В файле `kaspersky_cybertrace` укажите следующие строки:

```
/var/log/kaspersky_cyberTrace.log
{
# save 3 months of logs
rotate 3
monthly
missingok
notifempty
compress
delaycompress
sharedscripts
# run a script after log rotation
postrotate
invoke-rc.d rsyslog rotate > /dev/null
endscript
}
```

   c. Сохраните и закройте файл `kaspersky_cybertrace`.

   > Если требуется сохранить журналы за другой период, см. информацию о настройке файла `kaspersky_cybertrace` в документации по logrotate.

   После выполнения этой процедуры устройство Kaspersky CyberTrace будет добавлено в AlienVault USM / OSSIM.

Служба rsyslog будет сохранять события из Kaspersky CyberTrace в файле `/var/log/kaspersky_cyberTrace.log`.

После настройки Kaspersky CyberTrace и AlienVault USM / OSSIM выполните проверку работоспособности. Для этого отправьте события, используемые в проверке работоспособности, в Kaspersky CyberTrace с помощью утилиты Log Scanner (является частью Kaspersky CyberTrace). События для проверки работоспособности содержатся в файле `verification/kl_verification_test.txt`. Результат проверки можно просмотреть в веб-интерфейсе AlienVault USM / OSSIM.

По умолчанию каждое событие обнаружения для каждого потока данных об угрозах Kaspersky Threat Data Feed имеет свой тип в AlienVault. Остальные события обнаружения имеют значение `Kaspersky CyberTrace - Detection event` в поле `event name`.

Вы можете переименовать события обнаружения импортированных потоков данных об угрозах, чтобы классифицировать события обнаружения по их категориям.

Чтобы переименовать события обнаружения импортированного потока данных об угрозах, выполните следующие действия:

1. Добавьте следующую строку в раздел `translation` файла конфигурации `/etc/ossim/agent/plugins/kaspersky_cyberTrace.cfg`:

   `%CATEGORY_ATTRIBUTE_VALUE_OF_THE_IMPORTED_FEED%=%ANY_FREE_NUMERIC_VALUE%`

   где `%CATEGORY_ATTRIBUTE_VALUE_OF_THE_IMPORTED_FEED%` – значение атрибута категории импортированного потока данных об угрозах из `kl_feed_service.conf`. Например: `Custom_Feed = 50`.

2. Сохраните изменения и закройте файл.

3. Добавьте следующую строку перед последней строкой файла `/usr/share/doc/ossim-mysql/contrib/plugins/kaspersky_cyberTrace.sql`:

   ```
   (23021992, %NUMERIC_VALUE_SPECIFIED_AT_THE_kaspersky_cyberTrace.cfg%, 15, 71, NULL,
   'Kaspersky CyberTrace - %NAME_TO_REPLACE%', 5, 8),
   ```

4. Сохраните изменения и закройте файл.

5. Выполните следующую команду:

   ```
   cat /usr/share/doc/ossim-mysql/contrib/plugins/kaspersky_cyberTrace.sql | ossim-db
   /etc/init.d/ossim-agent restart
   /etc/init.d/ossim-server restart
   ```

Просмотр событий Kaspersky CyberTrace в AlienVault USM / OSSIM

В этом разделе описано, как просматривать события Kaspersky CyberTrace в AlienVault USM / OSSIM.

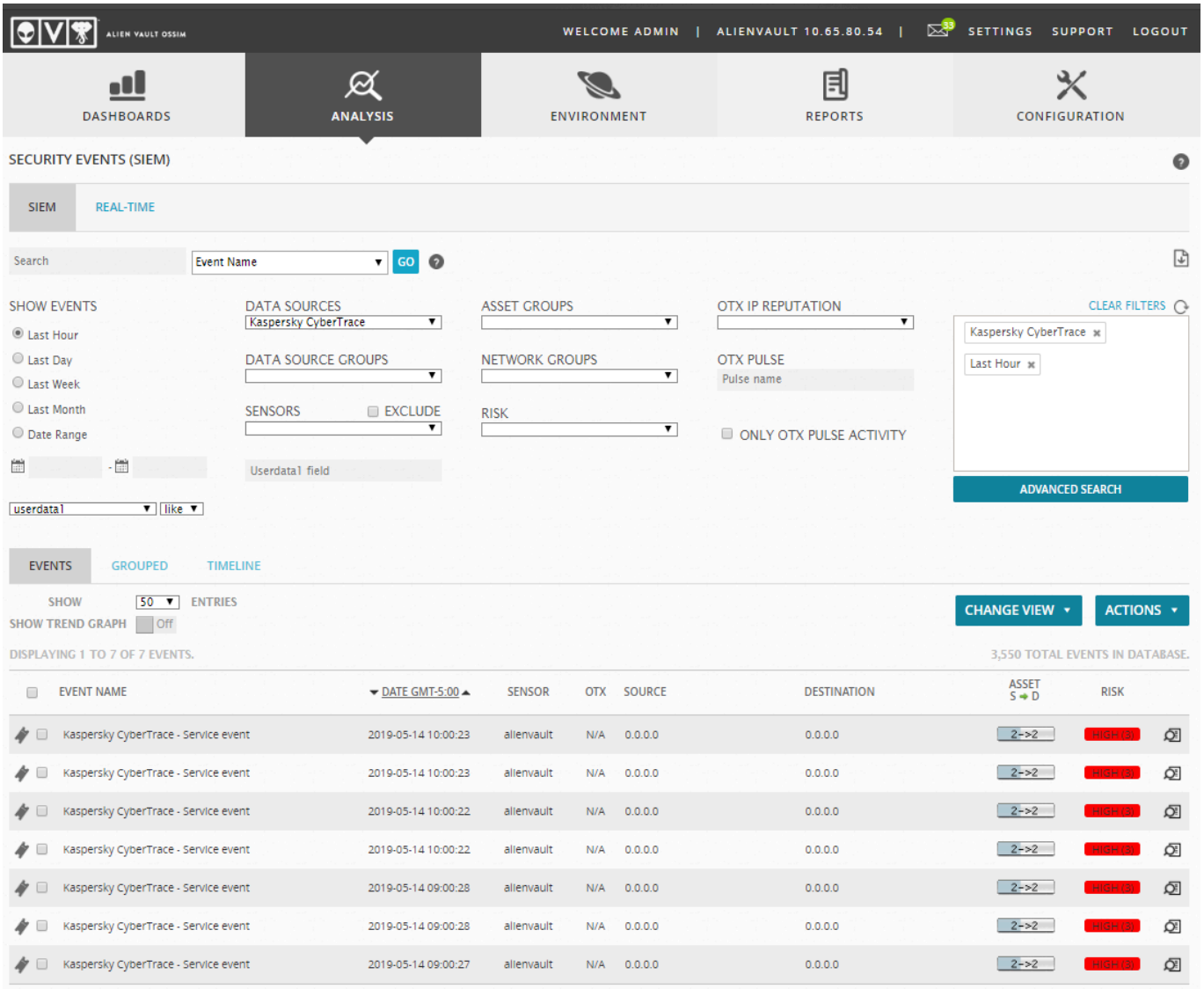
Чтобы просмотреть события Kaspersky CyberTrace в веб-интерфейсе AlienVault USM / OSSIM, выполните следующие действия:

1. В браузере откройте веб-интерфейс AlienVault USM / OSSIM.

2. Выберите **Analysis** → **Security events (SIEM)**.

3. В раскрывающемся списке **Data Sources** выберите **Kaspersky CyberTrace**.

AlienVault USM / OSSIM покажет события, полученные из Kaspersky CyberTrace.



События, полученные из Kaspersky CyberTrace

AlienVault USM / OSSIM показывает события Kaspersky CyberTrace двух типов, которые указаны в столбце **Event Name** списка событий:

- Служебные события

  Нажмите на кнопку в последнем столбце таблицы. Для служебных событий отображаются следующие данные (как показано на рисунке ниже):

  - Поле **Userdata1** содержит само событие службы.
  - Поле **Userdata2** содержит контекст события, если таковой имеется.

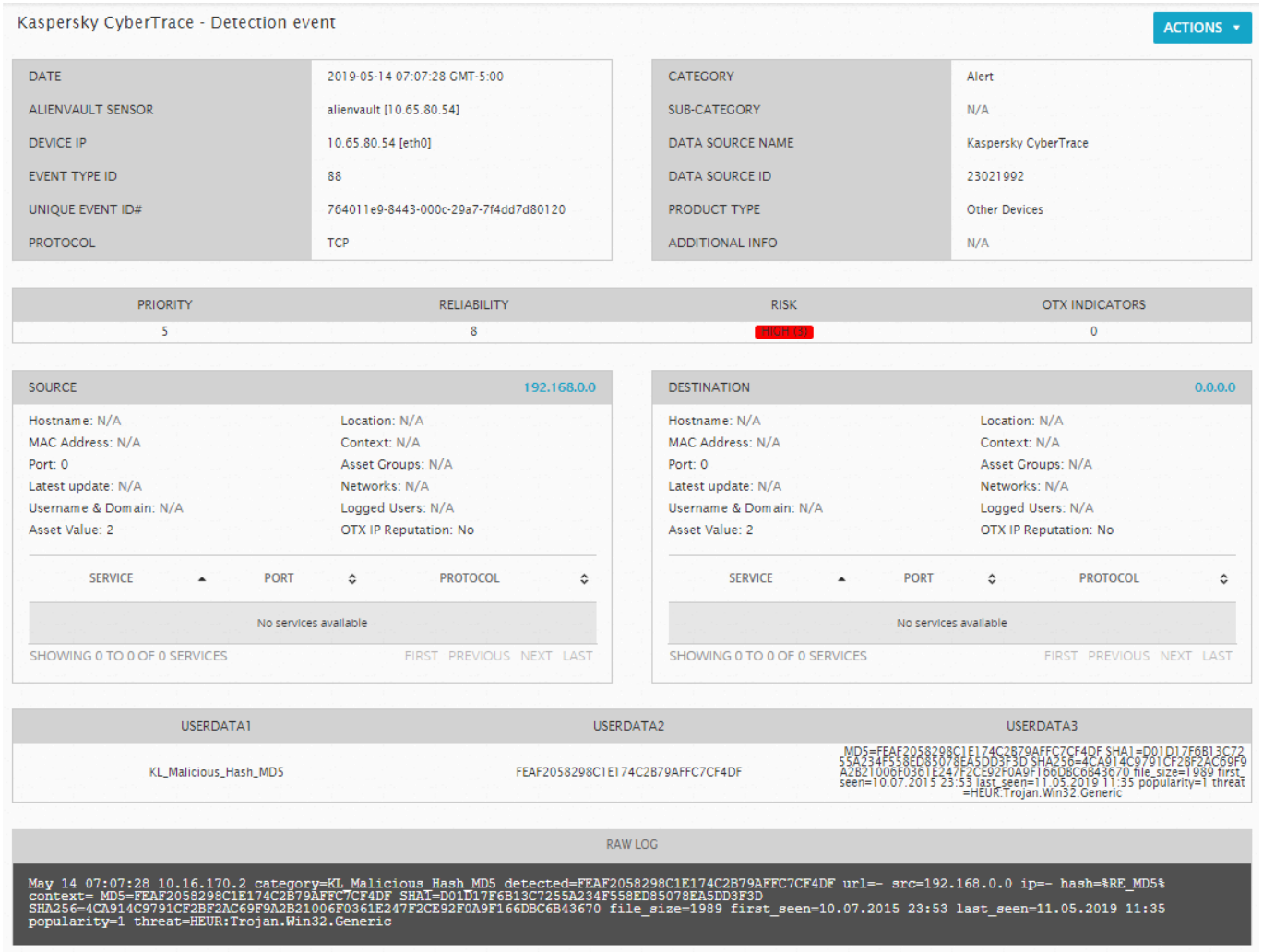
- События обнаружения

  Нажмите на кнопку в последнем столбце таблицы. Для событий обнаружения отображаются следующие данные (как показано на рисунке ниже):

  - Поле **Userdata1** содержит поток данных об угрозах, который использовался в процессе обнаружения.
  - Поле **Userdata2** содержит обнаруженный индикатор.

- Поле **Userdata3** содержит контекст записи потока данных, вовлеченной в процесс обнаружения киберугроз.

  Поле **Userdata3** содержит до 1024 символов, поэтому оно может не содержать весь контекст. Все событие (включая контекст) содержится в поле **RAW LOG**.



Данные события обнаружения

Интеграция с FortiSIEM

В этой главе описывается, как интегрировать потоки данных об угрозах Kaspersky Threat Data Feeds с таким программным обеспечением для управления информацией и событиями безопасности (SIEM), как FortiSIEM.

Мы рекомендуем интегрировать потоки данных об угрозах Kaspersky Threat Data Feeds с FortiSIEM с помощью Kaspersky CyberTrace.

Шаги интеграции с FortiSIEM

В этом разделе описываются шаги для интеграции Kaspersky CyberTrace с FortiSIEM.

Инструкции по интеграции, представленные в настоящем документе, применимы к FortiSIEM версии 5.2.

Чтобы интегрировать Kaspersky CyberTrace с FortiSIEM, выполните следующие действия:

1. Настройте Kaspersky CyberTrace для интеграции с ArcSight.
2. Настройте пересылку событий из FortiSIEM в Kaspersky CyberTrace.
3. Настройте отправку событий из Kaspersky CyberTrace и их получение в FortiSIEM.

После этого можно просматривать события, полученные из Kaspersky CyberTrace, в FortiSIEM.

Настройка Kaspersky CyberTrace для интеграции с FortiSIEM

В этом разделе описывается порядок настройки Kaspersky CyberTrace для интеграции с FortiSIEM.

Чтобы настроить Kaspersky CyberTrace для интеграции с FortiSIEM, выполните следующие действия:

1. Загрузите Kaspersky CyberTrace со страницы https://support.kaspersky.com/datafeeds/download/15920.
2. Установка Kaspersky CyberTrace.
   - В ОС Linux Kaspersky CyberTrace устанавливается в каталог `/opt/kaspersky/ktfs`.
   - В случае установки в ОС Windows каталог установки в дальнейшем называется `%CyberTrace_installDir%`.
3. Откройте файл конфигурации kl_feed_service.conf для редактирования.
   - В Linux файл kl_feed_service.conf находится в каталоге `/opt/kaspersky/ktfs/etc`.
   - В Windows файл kl_feed_service.conf находится в каталоге `%CyberTrace_installDir%\bin`.

   Вы также можете настроить Kaspersky CyberTrace и задать параметры, описанные в этом разделе, с помощью веб-интерфейса Kaspersky CyberTrace.
4. Убедитесь, что элемент `Configuration > InputSettings > ConnectionString` содержит IP-адрес сервера, на котором будет выполняться Kaspersky CyberTrace, и незанятый порт (например, `9999`). IP-адрес и порт должны быть указаны в формате `%IP_address%:%port%` (например, `10.43.11.15:9999`).
5. В файле kl_feed_service.conf добавьте следующие элементы в элемент `Configuration > InputSetting > RegExps > Source id="default"`:

   ```
   <Device type="CONTEXT">[^\|]*\|([^\|]*\|[^\|]*)\|</Device>
   <DeviceIp type="CONTEXT" concatenate="#1">dvc\=(\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3})(?:$|\s|\,)</DeviceIp>
   <UserName type="CONTEXT">user\=(.*?)(?:$|\s|\,)</UserName>
   <DeviceAction type="CONTEXT">act=(.*?)(?:$|\s|\,)</DeviceAction>
   ```

6. В элементе `Configuration > OutputSettings > AlertFormat` укажите следующее значение:

   ```
   <![CDATA[Kaspersky Lab|Kaspersky CyberTrace|1.0|1|4|alert=%Alert%;msg=%RecordContext%]]>
   ```

   Если вы используете веб-интерфейс Kaspersky CyberTrace для указания этого значения, опустите `<![CDATA[` в начале и `]]>` в конце значения.

7. В элементе `Configuration > OutputSettings > EventFormat` укажите следующее значение:

```
<![CDATA[Kaspersky Lab|Kaspersky
CyberTrace|1.0|2|8|reason=%Category%;detected=%MatchedIndicator%;act=%DeviceAction%;dst=%RE_IP%;src=%SRC_IP%;md5
```

Если вы используете веб-интерфейс Kaspersky CyberTrace для указания этого значения, опустите `<![CDATA[` в начале и `]]>` в конце значения.

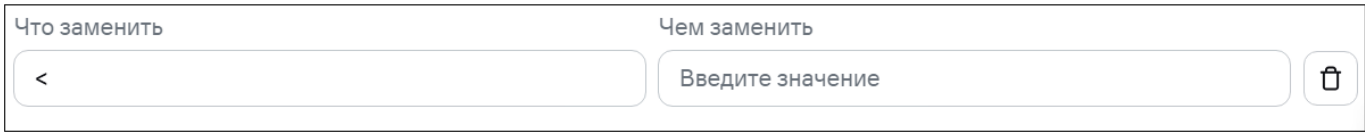
8. В элементе `Configuration > OutputSettings > ConnectionString` укажите IP-адрес экземпляра FortiSIEM, которому Kaspersky CyberTrace будет отправлять события обнаружения, и порт `514`.

   Укажите IP-адрес и порт в формате `%IP_address%:%port%` (например, `10.43.11.43:514`).

9. В элементе `Configuration > NormalizingRules` укажите следующее правило:

   ```
   <Replace input="&lt;" output="&#10;&lt;" />
   ```

   Вы также можете создать это правило с помощью веб-интерфейса Kaspersky CyberTrace следующим образом:



Правило нормализации для событий FortiSIEM

10. Перезапустите службу Kaspersky CyberTrace (один из модулей Kaspersky CyberTrace), выполнив следующую команду:

    - `/opt/kaspersky/ktfs/etc/init.d/kl_feed_service restart` (в Linux)
    - `%CyberTrace_installDir%\bin\kl_control.bat restart` (в Windows)

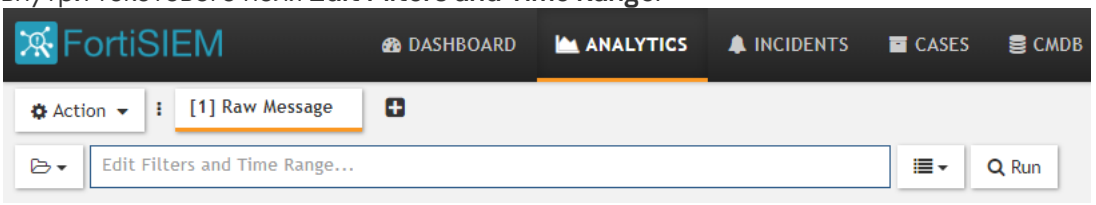
Просмотр формата пересылаемых событий в FortiSIEM

В описанной выше процедуре предполагается, что для извлечения IP-адресов, URL-адресов и хешей из событий, отправленных из FortiSIEM, используются универсальные регулярные выражения. Возможно, вам придется изменить эти и другие регулярные выражения в зависимости от формата событий. Например, это может потребоваться для извлечения из события имени пользователя или других данных, которые позже будут вставлены в событие обнаружения и отправлены в FortiSIEM. Перед редактированием существующих регулярных выражений или добавлением новых вам необходимо проанализировать исходные события, поступившие в Kaspersky CyberTrace.

Вы также можете просматривать эти события в веб-интерфейсе Kaspersky CyberTrace. После настройки пересылки событий в FortiSIEM в веб-интерфейсе Kaspersky CyberTrace выберите страницу **Параметры** → **Источники событий**, затем нажмите кнопку (**Изменить**) рядом с требуемым источником событий. В результате в разделе **Свойства** в окне свойств отображаемого источника событий будут отображаться события, поступающие в Kaspersky CyberTrace.

Чтобы просмотреть формат событий в FortiSIEM, выполните следующие действия:

1. В веб-консоли FortiSIEM выберите вкладку **Analytics**.
2. Щелкните внутри текстового поля **Edit Filters and Time Range**.

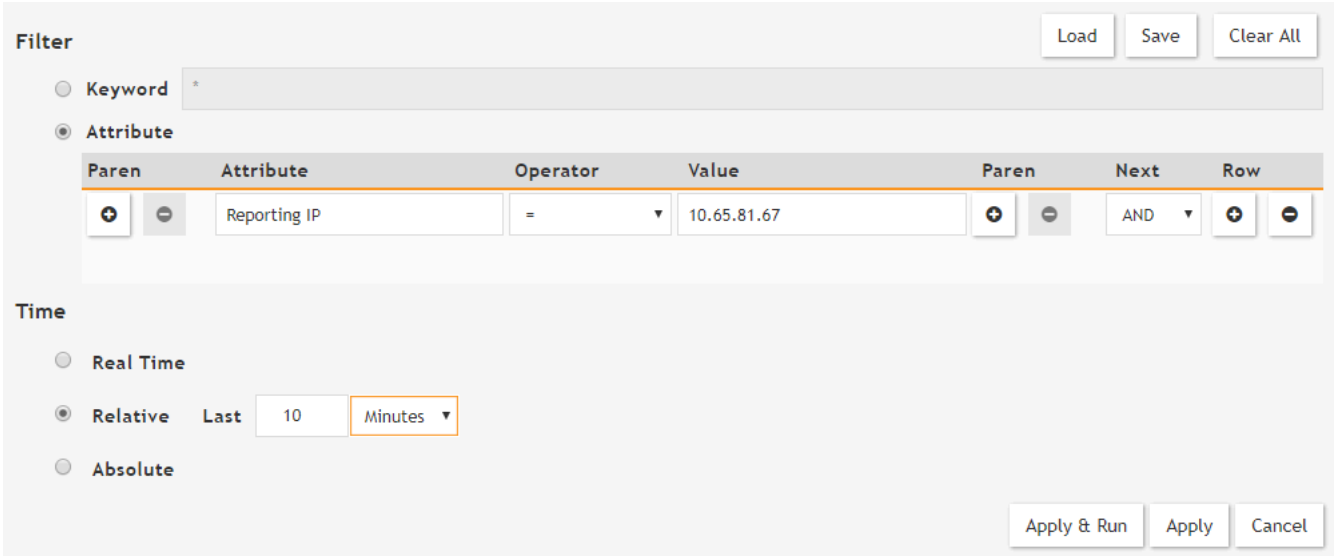


Выбор событий FortiSIEM

Появится форма **Filters**, в которой можно задать фильтр и временной диапазон для событий.

3. Укажите фильтр для нужных событий.

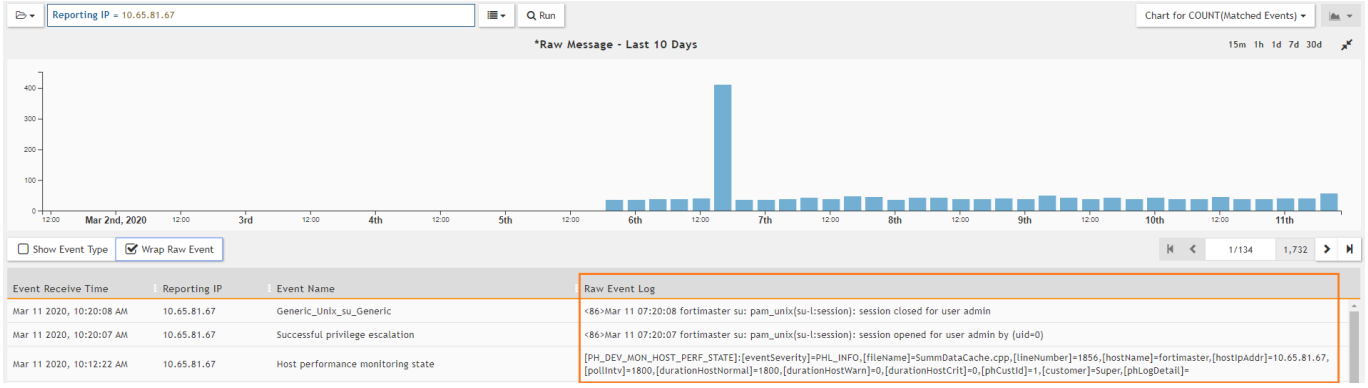
   Например, можно указать IP-адрес устройства, с которого приходят события в FortiSIEM (атрибут `Reporting IP`). Также в группе настроек **Time** можно задать временной диапазон для событий (например, последние 10 минут) или указать, что события должны отображаться в режиме реального времени.



Настройка фильтра для событий FortiSIEM

4. Нажмите на кнопку **Save & Run**.

   Столбец **Raw Event Log** содержит события в том же формате, в котором они пересылаются из FortiSIEM в Kaspersky CyberTrace.



Отображаемые события FortiSIEM

Настройка пересылки событий из FortiSIEM

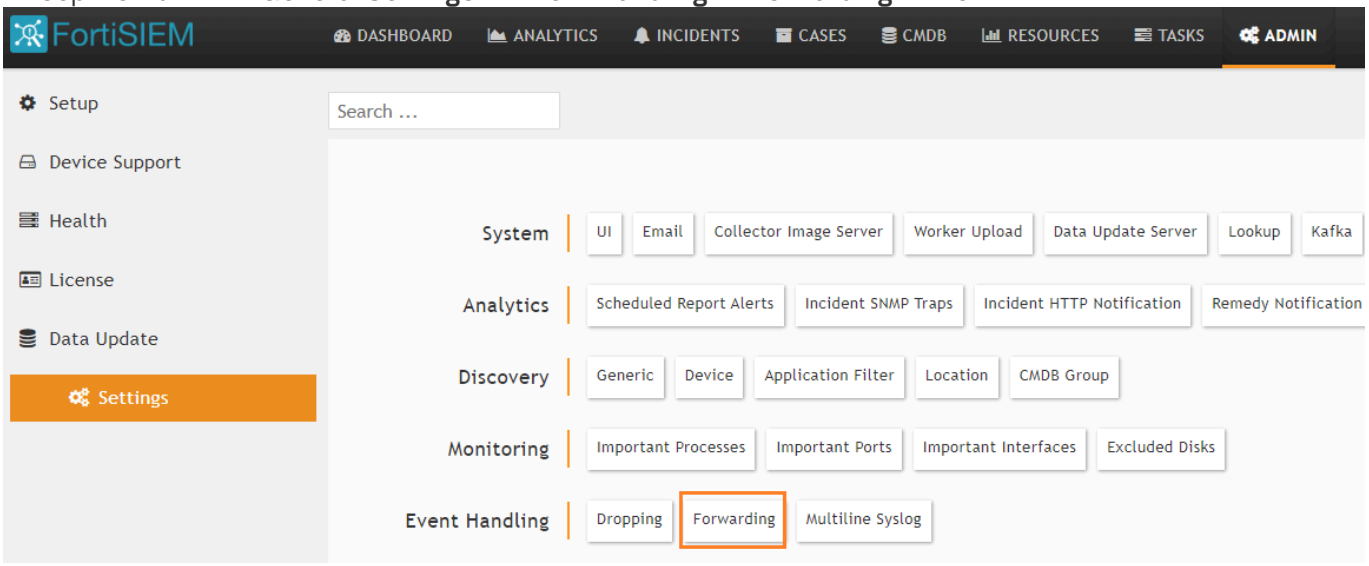
В этом разделе описывается порядок настройки пересылки событий из FortiSIEM в Kaspersky CyberTrace.

Чтобы настроить пересылку событий из FortiSIEM в Kaspersky CyberTrace, выполните следующие действия:

1. Откройте веб-консоль FortiSIEM.

   Используемая учетная запись FortiSIEM должна иметь права администратора.

2. Выберите **Admin** → **General Settings** → **Event Handling** → **Forwarding** → **New**.



Создание нового правила пересылки

   Откроется окно **Event Forwarding Rule**.

3. Задайте параметры пересылки событий:

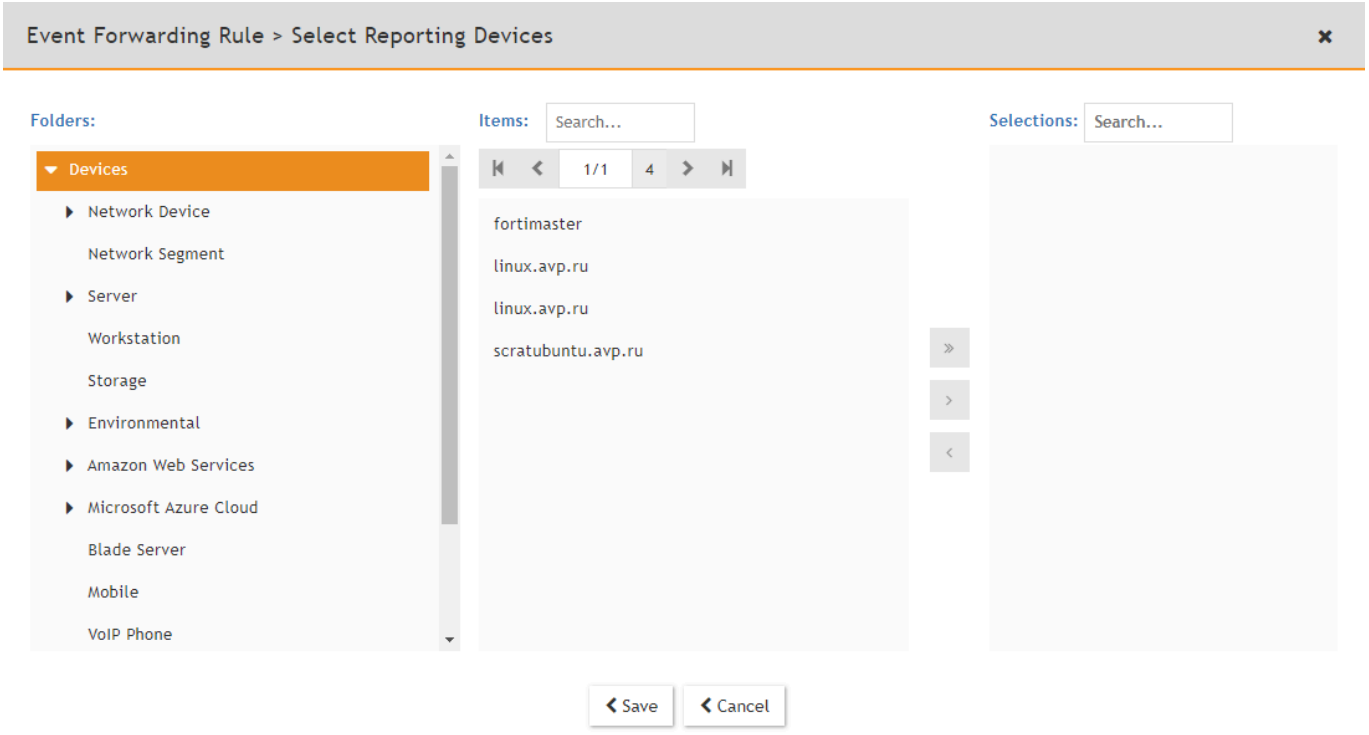
   - В поле **Reporting Device** укажите устройства, с которых необходимо пересылать события в Kaspersky CyberTrace. Можно выбрать вариант **All**, чтобы указать, что события с каждого устройства должны пересылаться в Kaspersky CyberTrace.

     - Для выбора других вариантов нажмите на стрелку вниз, чтобы открыть окно **Event Dropping Rule** → **Select Reporting Devices**, и выберите нужные значения на панелях **Folders**, **Items** и **Selections**.

     Поле **Reporting Device** не должно быть пустым.

- В поле **Event type** укажите типы событий, которые необходимо пересылать в Kaspersky CyberTrace. Можно выбрать вариант **All**, чтобы указать, что события каждого типа должны пересылаться в Kaspersky CyberTrace.

  - Для выбора других вариантов нажмите на стрелку вниз, чтобы открыть окно **Event Forwarding Rule → Select Event Types**, и выберите нужные значения на панелях **Folders**, **Items** и **Selections**.



Выбор типов событий

Поле **Event type** не должно быть пустым.

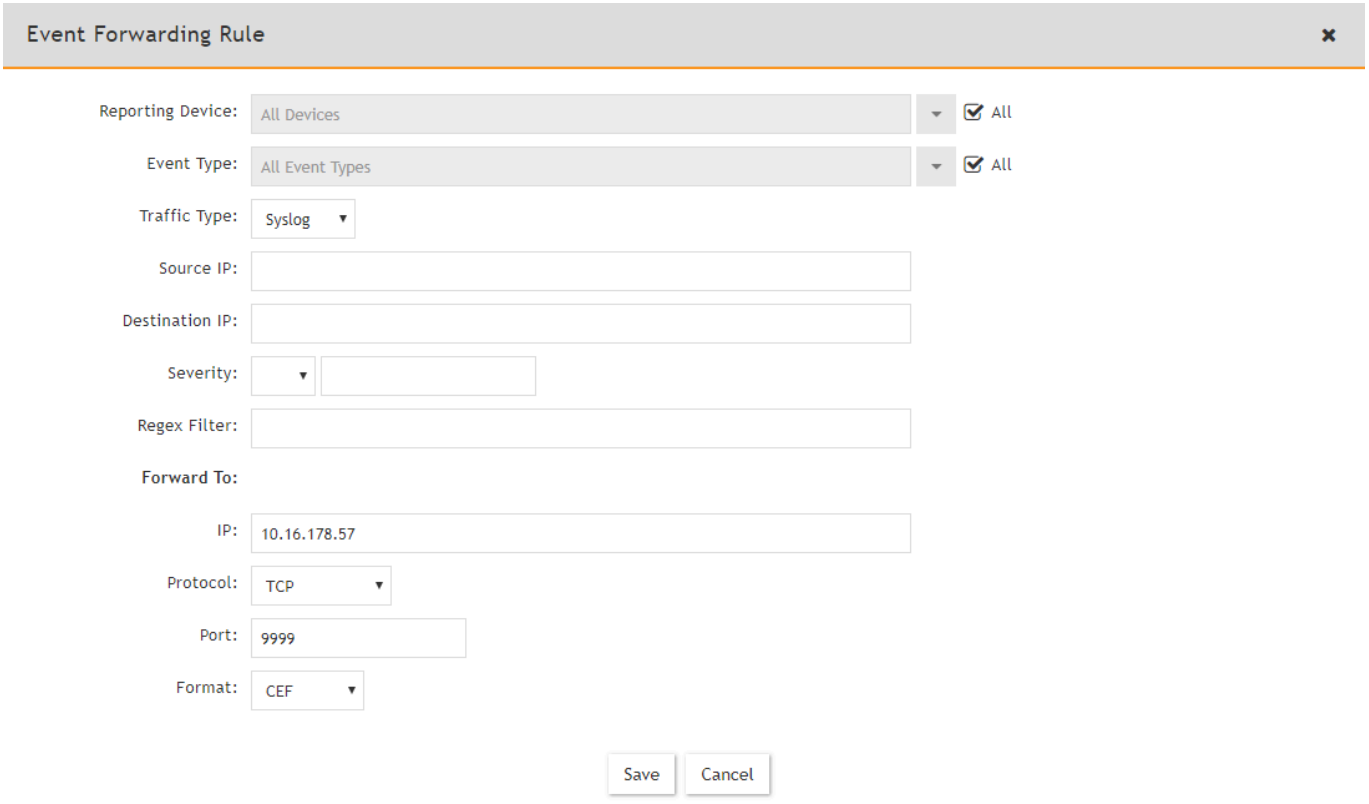
- В поле **Traffic Type** выберите **Syslog**.
- В поле **Source IP** можно указать значение, которое должно присутствовать во всех пересылаемых событиях в соответствующем поле.
- В поле **Destination IP** можно указать значение, которое должно присутствовать во всех пересылаемых событиях в соответствующем поле.
- В полях **Severity** можно указать желаемую важность событий.
- В поле **Regex Filter** можно указать регулярное выражение, которому должны соответствовать пересылаемые события.
- В поле **Forwarding Protocol** выберите **TCP**.
- В поле **Forwarding to IP** укажите IP-адрес сервера, на котором выполняется Kaspersky CyberTrace.

  Этот IP-адрес указывается в элементе `InputSettings > ConnectionString` файла конфигурации kl_feed_service.conf.

- В поле **Forwarding to Port** укажите порт сервера, на котором выполняется Kaspersky CyberTrace.

  Этот порт указывается в элементе `InputSettings > ConnectionString` файла конфигурации kl_feed_service.conf.

- В поле **Format** выберите **CEF**.

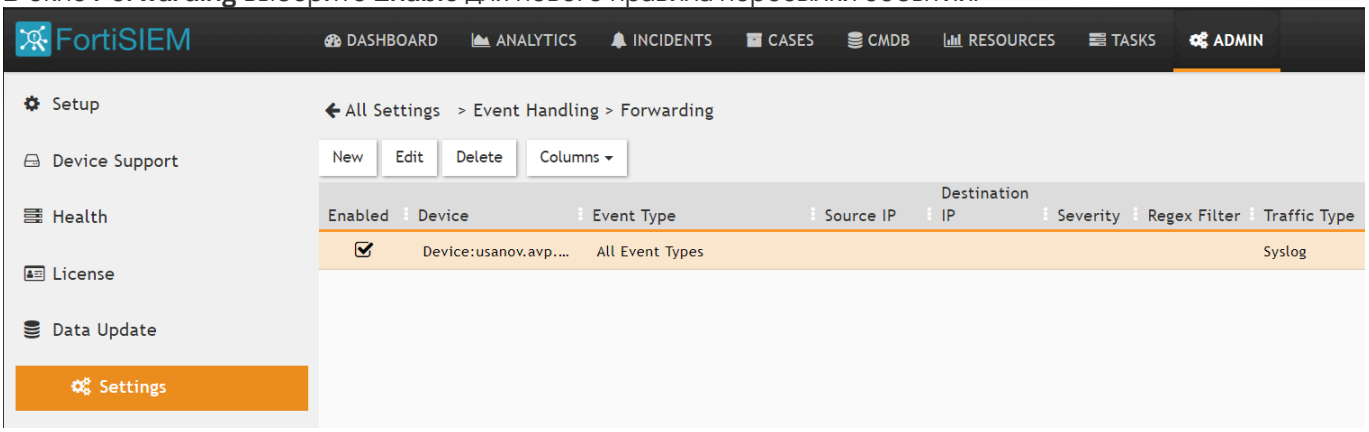


Окно **Event Forwarding Rule**

4. Нажмите на кнопку **Save**.

   Окно **Event Forwarding Rule** закроется, а в окне **Forwarding** отобразится новое правило пересылки событий.

5. В окне **Forwarding** выберите **Enable** для нового правила пересылки событий.



Окно **Event Forwarding Rule**

Получение событий из Kaspersky CyberTrace в FortiSIEM

В этом разделе описывается порядок настройки Kaspersky CyberTrace и FortiSIEM для того, чтобы приложение FortiSIEM получало события из Kaspersky CyberTrace.

Чтобы получать события из Kaspersky CyberTrace в FortiSIEM, выполните следующие действия:

1. Добавьте Kaspersky CyberTrace в FortiSIEM в качестве источника событий.
2. В FortiSIEM добавьте поля `Device IP Address` и `Detected indicator`.
3. В FortiSIEM добавьте правила парсинга событий из Kaspersky CyberTrace.
4. При желании в FortiSIEM можно добавить описания событий из Kaspersky CyberTrace.

Добавление Kaspersky CyberTrace в качестве источника событий в FortiSIEM

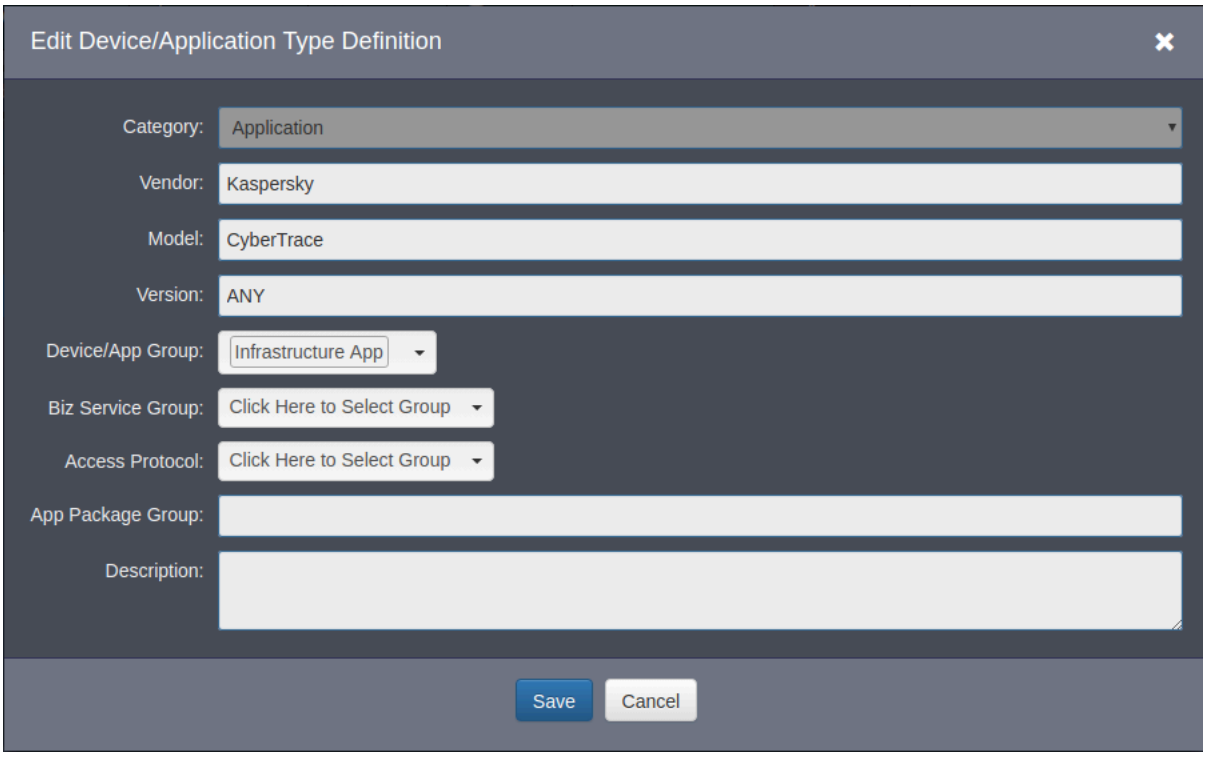
В этом разделе описывается порядок добавления Kaspersky CyberTrace в качестве источника событий в FortiSIEM.

Чтобы добавить Kaspersky CyberTrace в качестве источника событий, выполните следующие действия:

1. Откройте веб-консоль FortiSIEM.
2. Выберите **Admin** → **Device Support** → **Device/App**.
3. Нажмите на кнопку **New**.

   Откроется окно **Device/Application Type Definition**.
4. Укажите следующую информацию:
   - В поле **Category** выберите **Application**.
   - В поле **Vendor** укажите **Kaspersky**.
   - В поле **Model** укажите **CyberTrace**.
   - В поле **Version** укажите **ANY**.
   - В поле **Device/App Group** выберите **Applications** → **Infrastructure App**.

- Не изменяйте поле **Biz Service Group**.
- Снимите флажки для всех выбранных элементов в раскрывающемся списке в поле **Access Protocol**.



Редактирование определения типа устройства/приложения

5. Нажмите на кнопку **Save**.

   В списке поддерживаемых устройств и приложений появится новый элемент.

6. Нажмите на кнопку **Apply**.

Добавление полей в FortiSIEM

По умолчанию оповещение об обнаружении индикаторов компрометации, отправляемое Kaspersky CyberTrace, содержит IP-адрес устройства, отправившего исходное событие, и поле для обнаруженного индикатора. Однако FortiSIEM не содержит полей для сохранения этого IP-адреса и индикатора. В этом разделе описывается, как добавить поле для сохранения требуемых значений в FortiSIEM.

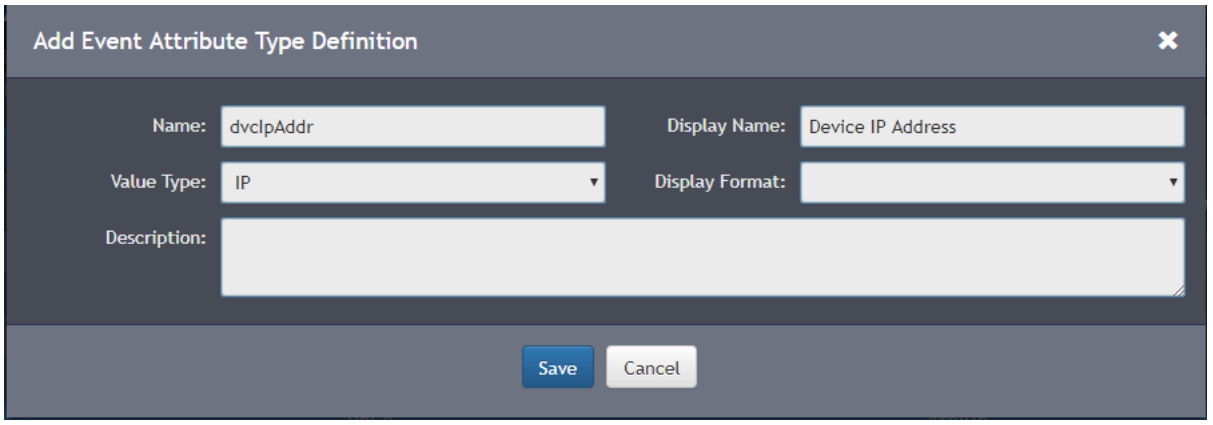
Чтобы добавить поле для сохранения IP-адреса и обнаруженного индикатора в FortiSIEM, выполните следующие действия:

1. Откройте веб-консоль FortiSIEM.
2. Выберите **Admin** → **Device Support** → **Event Attribute**.
3. Нажмите на кнопку **New**.

   Откроется окно **Add Event Attribute Type Definition**.

4. Укажите следующую информацию:
   - В поле **Name** укажите **dvcIpAddr**.
   - В поле **Display Name** укажите **IP-адрес устройства**.

- В поле **Value Type** выберите **IP**.
- Заполните остальные поля по своему усмотрению.



Добавление нового поля в FortiSIEM

5. Нажмите на кнопку **Save**.
6. Нажмите на кнопку **New**.
7. В открывшемся окне **Add Event Attribute Type Definition** укажите следующую информацию:
   - В поле **Name**, укажите **detectedIndicator**.
   - В поле **Display Name** укажите **Detected indicator**.
   - В поле **Value Type** выберите **String**.
   - Заполните остальные поля по своему усмотрению.
8. Нажмите на кнопку **Save**.
9. Нажмите на кнопку **Apply**.

Добавление правил парсинга событий из Kaspersky CyberTrace в FortiSIEM

В этом разделе описывается порядок добавления в FortiSIEM правил парсинга событий, поступающих из Kaspersky CyberTrace.

Чтобы добавить в FortiSIEM правила парсинга событий, выполните следующие действия:

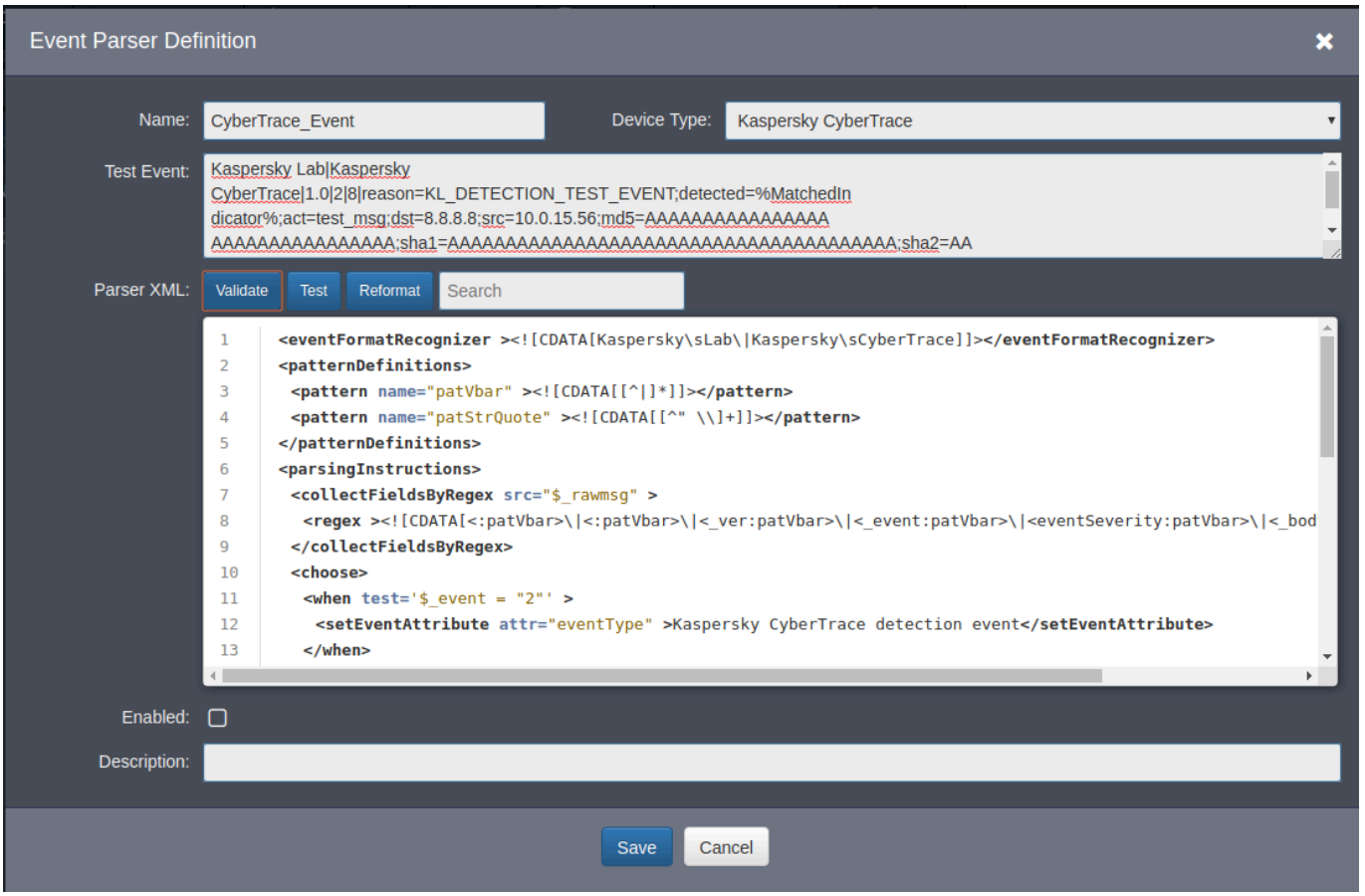
1. Откройте веб-консоль FortiSIEM.
2. Выберите **Admin** → **Device Support** → **Parser**.
3. Выберите парсер, после которого требуется добавить новый, и нажмите **New**.
   Откроется окно **Event Parser Definition**.
4. Укажите следующие значения:
   - В поле **Name**, укажите **CyberTrace_Event**.
   - В поле **Device Type** выберите **Kaspersky CyberTrace**.
   - В поле **Test Event** укажите следующее значение:

```
Kaspersky Lab|Kaspersky
CyberTrace|1.0|2|8|reason=KL_DETECTION_TEST_EVENT;detected=%MatchedIndicator%;act=test_msg;dst=8.8.8.8;src=1
and_more:true
Kaspersky Lab|Kaspersky CyberTrace|1.0|1|4|alert=KL_TEST_ALERT;msg=there_is_some_context:true and_more:true
```

- В поле **Parser XML** укажите следующее значение:

```
<eventFormatRecognizer>
  <![CDATA[Kaspersky\sLab\|Kaspersky\sCyberTrace]]>
</eventFormatRecognizer>
 <patternDefinitions>
 <pattern name="patVbar" ><![CDATA[[^|]*]]></pattern>
 <pattern name="patStrQuote" ><![CDATA[[^" \\]+]]></pattern>
 </patternDefinitions>
 <parsingInstructions>
 <collectFieldsByRegex src="$_rawmsg" >
 <regex>
  <![CDATA[<:patVbar>\|<:patVbar>\|<_ver:patVbar>\|<_event:patVbar>\|
<eventSeverity:patVbar>\|<_body:gPatMesgBody>]]>
 </regex>
 </collectFieldsByRegex>
 <choose>
 <when test='$_event = "2"' >
 <setEventAttribute attr="eventType" >Kaspersky CyberTrace detection
event</setEventAttribute>
 </when>
 <when test='$_event = "1"' >
 <setEventAttribute attr="eventType" >Kaspersky CyberTrace service
event</setEventAttribute>
 </when>
 </choose>
 <collectFieldsByKeyValuePair kvsep="=" sep=";" src="$_body" >
 <attrKeyMap attr="alertName" key="alert" />
 <attrKeyMap attr="threatCategory" key="reason" />
 <attrKeyMap attr="detectedIndicator" key="detected" />
 <attrKeyMap attr="srcAction" key="act" />
 <attrKeyMap attr="destIpAddr" key="dst" />
 <attrKeyMap attr="srcIpAddr" key="src" />
 <attrKeyMap attr="hashMD5" key="md5" />
 <attrKeyMap attr="hashSHA1" key="sha1" />
 <attrKeyMap attr="hashSHA2" key="sha2" />
 <attrKeyMap attr="uriQuery" key="request" />
 <attrKeyMap attr="dvcIpAddr" key="dvc" />
 <attrKeyMap attr="serviceName" key="sourceServiceName" />
 <attrKeyMap attr="user" key="suser" />
 <attrKeyMap attr="msg" key="msg" />
 </collectFieldsByKeyValuePair>
 </parsingInstructions>
```

Если вы добавили новые регулярные выражения и изменили формат событий обнаружения в файле конфигурации kl_feed_service.conf, укажите новый формат событий обнаружения в поле **Test Event**. Кроме того, в поле **Parser XML** в элементе `collectFieldsByKeyValuePair` добавьте правила соответствия между полями событий из Kaspersky CyberTrace и полями FortiSIEM, в которых должны сохраняться значения этих полей событий. Правила соответствия должны иметь следующий формат: `<attrKeyMap attr="%FortiSIEM_field%" key="%Kaspersky_CyberTrace_field%" />`.



Редактирование определения парсера

5. Нажмите кнопку **Reformat**.
6. Нажмите кнопку **Validate**, чтобы проверить XML-данные в поле **Parser XML**.

   Отобразится сообщение с результатом проверки.
7. Нажмите кнопку **Test**.

   Откроется окно для проверки введенных данных.
8. В окне **Test Event Parser** нажмите кнопку **Test**.

   Если в столбце **Errors** появляются сообщения об ошибках, выполните следующие действия:

   a. Приведите в соответствие поля **Test Event** и **Parser XML**.

   b. Нажмите на кнопку **Back** и укажите правильные данные в полях **Test Event** и **Parser XML**.

   c. Еще раз проверьте данные.
9. Нажмите на кнопку **Back**.
10. В окне **Event Parser Definition** установите флажок **Enabled**.
11. Нажмите на кнопку **Save**.
12. В разделе **Admin** → **Device Support** → **Parser** нажмите **Apply**, а в открывшемся окне сообщения нажмите **Yes**, чтобы согласиться с изменениями.

Добавление описаний событий в FortiSIEM

В этом разделе объясняется, как добавлять описания к событиям обнаружения и событиям службы, отправляемым Kaspersky CyberTrace.

Чтобы добавить описания к событиям из Kaspersky CyberTrace, выполните следующие действия:

1. Откройте веб-консоль FortiSIEM.
2. Выберите **Admin** → **Device Support** → **Event** → **New**.

   Откроется окно **Event Definition**.
3. Укажите следующие данные:
   - В поле **Name** укажите **PH_DEV_MON_CUST_CYBERTRACE_DETECTION_EVENT**.
   - В поле **Device Type** выберите **Kaspersky CyberTrace**.
   - В поле **Event Type Group** выберите **Security**.
   - В поле **Severity** выберите **8-MEDIUM**.
   - В поле **Description** укажите **События обнаружения из Kaspersky CyberTrace**.
4. Нажмите на кнопку **Сохранить**.
5. Выберите **Admin** → **Device Support** → **Event** → **New**.
6. В открывшемся окне **Event Definition** укажите следующие данные:
   - В поле **Name**, укажите **PH_DEV_MON_CUST_CYBERTRACE_SERVICE_EVENT**.
   - В поле **Device Type** выберите **Kaspersky CyberTrace**.
   - В поле **Event Type Group** выберите **Info**.
   - В поле **Severity** выберите **4-LOW**.
   - В поле **Description** укажите **События службы из Kaspersky CyberTrace**.
7. Нажмите на кнопку **Сохранить**.
8. В разделе **Admin** → **Device Support** → **Event** нажмите **Apply**, а в открывшемся окне сообщения нажмите **Yes**, чтобы согласиться с изменениями.

Отображение полей контекста в FortiSIEM

В этом разделе описывается, как отобразить поле контекста в событиях, которые FortiSIEM получает из Kaspersky CyberTrace. В качестве примера используется поле `threat_score`.

Можно вставлять некоторые поля в исходящие события отдельно от контекста записей потока данных об угрозах. Таким полям в исходящих событиях можно присваивать произвольные наименования. Эти поля называются *полями контекста*; их список содержится в элементе `ActionableFields` описания потока данных об угрозах в файле конфигурации kl_feed_service.conf.

Сначала нужно отредактировать файл конфигурации kl_feed_service.conf, чтобы сделать `threat_score` полем контекста в Kaspersky CyberTrace. Затем нужно отредактировать правила парсинга в FortiSIEM для правильного отображения событий из Kaspersky CyberTrace.

Редактирование конфигурационного файла kl_feed_service.conf

Чтобы сделать `threat_score` полем контекста в Kaspersky CyberTrace, выполните следующие действия:

1. Откройте файл конфигурации kl_feed_service.conf для редактирования.
   - В Linux файл kl_feed_service.conf находится в каталоге `/opt/kaspersky/ktfs/etc`.
   - В Windows файл kl_feed_service.conf находится в каталоге `%CyberTrace_installDir%\bin`.
2. В элементе `Configuration > OutputSettings > EventFormat` укажите следующее значение:
   ```
   <![CDATA[Kaspersky Lab|Kaspersky
   CyberTrace|1.0|2|8|reason=%Category%;detected=%MatchedIndicator%;act=%DeviceAction%;dst=%RE_IP%;src=%SRC_IP%;md5
   ```
3. В элементе `Configuration > OutputSettings > ActionableFieldContextFormat` укажите следующее значение:
   ```
   %ParamName%=%ParamValue%;
   ```
4. В элемент `<Feed filename="IP_Reputation_Data_Feed.json" enabled="true" type="default">` добавьте следующие данные:
   ```
   <ActionableFields>
       <ActionableField name="threat_score" output_name="kl_threat_score"/>
   </ActionableFields>
   ```
5. Сохраните файл kl_feed_service.conf.
6. Перезапустите службу Kaspersky CyberTrace (компонент Kaspersky CyberTrace), выполнив следующую команду:
   - `/opt/kaspersky/ktfs/etc/init.d/kl_feed_service restart` (в Linux)
   - `%CyberTrace_installDir%\bin\kl_control.bat restart` (в Windows)

Службу Kaspersky CyberTrace можно перенастроить и перезапустить с помощью веб-интерфейса Kaspersky CyberTrace.

Редактирование правил парсинга для событий из Kaspersky CyberTrace

Чтобы отредактировать в FortiSIEM правила парсинга событий из Kaspersky CyberTrace, выполните следующие действия:

1. Откройте веб-консоль FortiSIEM.
2. Выберите **Admin** → **Device Support** → **Parser**.
3. В списке парсеров откройте пункт **CyberTrace_Event**.

   Откроется окно **Event Parser Definition**, содержащее данные парсера `CyberTrace_Event`.
4. Измените данные следующим образом:
   - В поле **Test Event** укажите следующее значение:

```
Kaspersky Lab|Kaspersky
CyberTrace|1.0|2|8|reason=KL_DETECTION_TEST_EVENT;detected=%MatchedIndicator%;act=test_msg;dst=8.8.8.8;src=1
and_more:true
Kaspersky Lab|Kaspersky CyberTrace|1.0|1|4|alert=KL_TEST_ALERT;msg=there_is_some_context:true and_more:true
```

- В поле **Parser XML** укажите следующее значение:

```
<eventFormatRecognizer>
  <![CDATA[Kaspersky\sLab\|Kaspersky\sCyberTrace]]>
</eventFormatRecognizer>
 <patternDefinitions>
 <pattern name="patVbar" ><![CDATA[[^|]*]]></pattern>
 <pattern name="patStrQuote" ><![CDATA[[^" \\]+]]></pattern>
 </patternDefinitions>
 <parsingInstructions>
 <collectFieldsByRegex src="$_rawmsg" >
 <regex>
  <![CDATA[<:patVbar>\|<:patVbar>\|<_ver:patVbar>\|<_event:patVbar>\|
<eventSeverity:patVbar>\|<_body:gPatMesgBody>]]>
 </regex>
 </collectFieldsByRegex>
 <choose>
 <when test='$_event = "2"' >
 <setEventAttribute attr="eventType" >Kaspersky CyberTrace detection
event</setEventAttribute>
 </when>
 <when test='$_event = "1"' >
 <setEventAttribute attr="eventType" >Kaspersky CyberTrace service
event</setEventAttribute>
 </when>
 </choose>
 <collectFieldsByKeyValuePair kvsep="=" sep=";" src="$_body" >
 <attrKeyMap attr="alertName" key="alert" />
 <attrKeyMap attr="threatCategory" key="reason" />
 <attrKeyMap attr="detectedIndicator" key="detected" />
 <attrKeyMap attr="srcAction" key="act" />
 <attrKeyMap attr="destIpAddr" key="dst" />
 <attrKeyMap attr="srcIpAddr" key="src" />
 <attrKeyMap attr="hashMD5" key="md5" />
 <attrKeyMap attr="hashSHA1" key="sha1" />
 <attrKeyMap attr="hashSHA2" key="sha2" />
 <attrKeyMap attr="uriQuery" key="request" />
 <attrKeyMap attr="dvcIpAddr" key="dvc" />
 <attrKeyMap attr="serviceName" key="sourceServiceName" />
 <attrKeyMap attr="user" key="suser" />
 <attrKeyMap attr="msg" key="msg" />
 <attrKeyMap attr="threatScore" key="kl_threat_score" />
 </collectFieldsByKeyValuePair>
 </parsingInstructions>
```

5. Нажмите на кнопку **Reformat**.

6. Нажмите на кнопку **Validate**, чтобы проверить XML-данные в поле **Parser XML**.

7. Нажмите на кнопку **Test**.

   Откроется окно для проверки введенных данных.

8. В окне **Test Event Parser** нажмите кнопку **Test**.

Если окно результатов проверки содержит сообщения об ошибках, выполните следующие действия:

a. Приведите в соответствие поля **Test Event** и **Parser XML**.

b. Нажмите на кнопку **Back** и укажите правильные данные в полях **Test Event** и **Parser XML**.

c. Еще раз проверьте данные.

9. Нажмите на кнопку **Back**.
10. В окне **Event Parser Definition** установите флажок **Enabled**.
11. Нажмите на кнопку **Save**.
12. В разделе **Admin** → **Device Support** → **Parser** нажмите **Apply**, а в открывшемся окне сообщения нажмите **Yes**, чтобы согласиться с изменениями.

Теперь события из Kaspersky CyberTrace корректно отображаются в FortiSIEM.

Поиск событий, полученных из Kaspersky CyberTrace, в FortiSIEM

В этом разделе описано, как просмотреть в FortiSIEM только те события, которые были получены из Kaspersky CyberTrace.

Чтобы просмотреть в FortiSIEM события, полученные из Kaspersky CyberTrace, выполните следующие действия:

1. Откройте веб-консоль FortiSIEM.
2. Выберите вкладку **Analytics**.
3. Щелкните внутри поля **Edit Filter and Time Range**.

   Появится форма **Filters**, в которой можно задать фильтр и временной диапазон для событий.
4. Укажите следующие условия фильтрации:
   - **Attribute**: `Reporting Vendor`
   - **Operator**: `=`
   - **Value**: `Kaspersky`
5. Нажмите на знак плюса (**+**) в столбце **Row**.
6. В новой строке задайте еще один фильтр:
   - **Attribute**: `Reporting Model`
   - **Operator**: `=`
   - **Value**: `CyberTrace`
7. В группе настроек **Time** укажите период, в течение которого нужные события поступали в FortiSIEM.

8. Нажмите на кнопку **Save & Run**.

   Теперь вкладка **Analysis** содержит только те события из Kaspersky CyberTrace, которые поступили за выбранный период.

Интеграция с другими решениями SIEM и не SIEM

В этом разделе описывается сопоставление имеющихся данных с потоками данных об угрозах в случаях, если SIEM-системы не используются или используется решение, которое Kaspersky CyberTrace пока не поддерживает.

Для сопоставления данных с потоками данных для угрозах можно использовать Log Scanner.

Проверка работоспособности (другие SIEM-системы и не-SIEM-системы)

В комплект поставки Kaspersky CyberTrace входят текстовые файлы в каталоге `verification`. Эти файлы можно использовать для проверки правильности интеграции Kaspersky CyberTrace в приложение-приемник событий.

Чтобы проверить правильность интеграции Kaspersky CyberTrace с приложением-приемником событий, выполните следующие действия:

1. Отправьте файл `kl_verification_test_cef.txt` из каталога `verification` в Kaspersky CyberTrace Service с помощью Log Scanner.

   В ОС Linux:

   ```
   ./log_scanner -p ../verification/kl_verification_test_cef.txt
   ```

   В ОС Windows:

   ```
   log_scanner.exe -p ..\verification\kl_verification_test_cef.txt
   ```

   Kaspersky CyberTrace Service проверит данные, содержащиеся во входном файле.

   > Если в этой команде указан флаг `-r`, результаты проверки будут записаны в файл отчета Log Scanner. Если флаг `-r` не указан, результаты проверки отправляются в приложение-приемник событий с использованием параметров для исходящих событий, указанных в служебных настройках Kaspersky CyberTrace.

2. Убедитесь, что приложение-приемник событий получило события в соответствии с таблицей ниже.

Результаты проверки работоспособности

Результаты проверки работоспособности зависят от используемых потоков данных об угрозах. В следующей таблице приведены целевые номера для проверки работоспособности при использовании всех коммерческих потоков данных об угрозах.

Результаты проверки работоспособности (коммерческие потоки данных об угрозах)

Используемый поток данных об угрозах	Значение eventName	Обнаруженные объекты
Malicious URL Data Feed	KL_Malicious_URL	http://fakess123.nu http://badb86360457963b90faac9ae17578ed.com
Phishing URL Data Feed	KL_Phishing_URL	http://fakess123ap.nu http://e77716a952f640b42e4371759a661663.com
Botnet C&C URL Data Feed	KL_BotnetCnC_URL	http://fakess123bn.nu http://a7396d61caffe18a4cffbb3b428c9b60.com
IP Reputation Data Feed	KL_IP_Reputation	192.0.2.0 192.0.2.3
Malicious Hash Data Feed	KL_Malicious_Hash_MD5	FEAF2058298C1E174C2B79AFFC7CF4DF 44D88612FEA8A8F36DE82E1278ABB02F C912705B4BBB14EC7E78FA8B370532C9
Mobile Malicious Hash Data Feed	KL_Mobile_Malicious_Hash_MD5	60300A92E1D0A55C7FDD360EE40A9DC1
Mobile Botnet C&C URL Data Feed	KL_Mobile_BotnetCnC_Hash_MD5	001F6251169E6916C455495050A3FB8D
Mobile Botnet C&C URL Data Feed	KL_Mobile_BotnetCnC_URL	http://sdfed7233dsfg93acvbhl.su/steallallsms.php
Ransomware URL Data Feed	KL_Ransomware_URL	http://fakess123r.nu http://fa7830b4811fbef1b187913665e6733c.com
APT URL Data Feed	KL_APT_URL	http://b046f5b25458638f6705d53539c79f62.com
APT Hash Data Feed	KL_APT_Hash_MD5	7A2E65A0F70EE0615EC0CA34240CF082
APT IP Data Feed	KL_APT_IP	192.0.2.4
IoT URL Data Feed	KL_IoT_URL	http://e593461621ee0f9134c632d00bf108fd.com/.i
ICS Hash Data Feed	KL_ICS_Hash_MD5	7A8F30B40C6564EFF95E678F7C43346C

В следующей таблице приведены целевые номера для проверки работоспособности при использовании только демонстрационных потоков данных об угрозах.

Результаты проверки работоспособности (демонстрационные потоки данных об угрозах)

Используемый поток данных об угрозах	Значение eventName	Обнаруженные объекты
DEMO Botnet_CnC_URL_Data_Feed	KL_BotnetCnC_URL	http://5a015004f9fc05290d87e86d69c4b237.com http://fakess123bn.nu
DEMO IP_Reputation_Data_Feed	KL_IP_Reputation	192.0.2.1 192.0.2.3
DEMO Malicious_Hash_Data_Feed	KL_Malicious_Hash_MD5	776735A8CA96DB15B422879DA599F474 FEAF2058298C1E174C2B79AFFC7CF4DF 44D88612FEA8A8F36DE82E1278ABB02F

Дополнительные сценарии установки (с использованием DMZ)

В этом разделе описываются дополнительные сценарии установки с использованием DMZ.

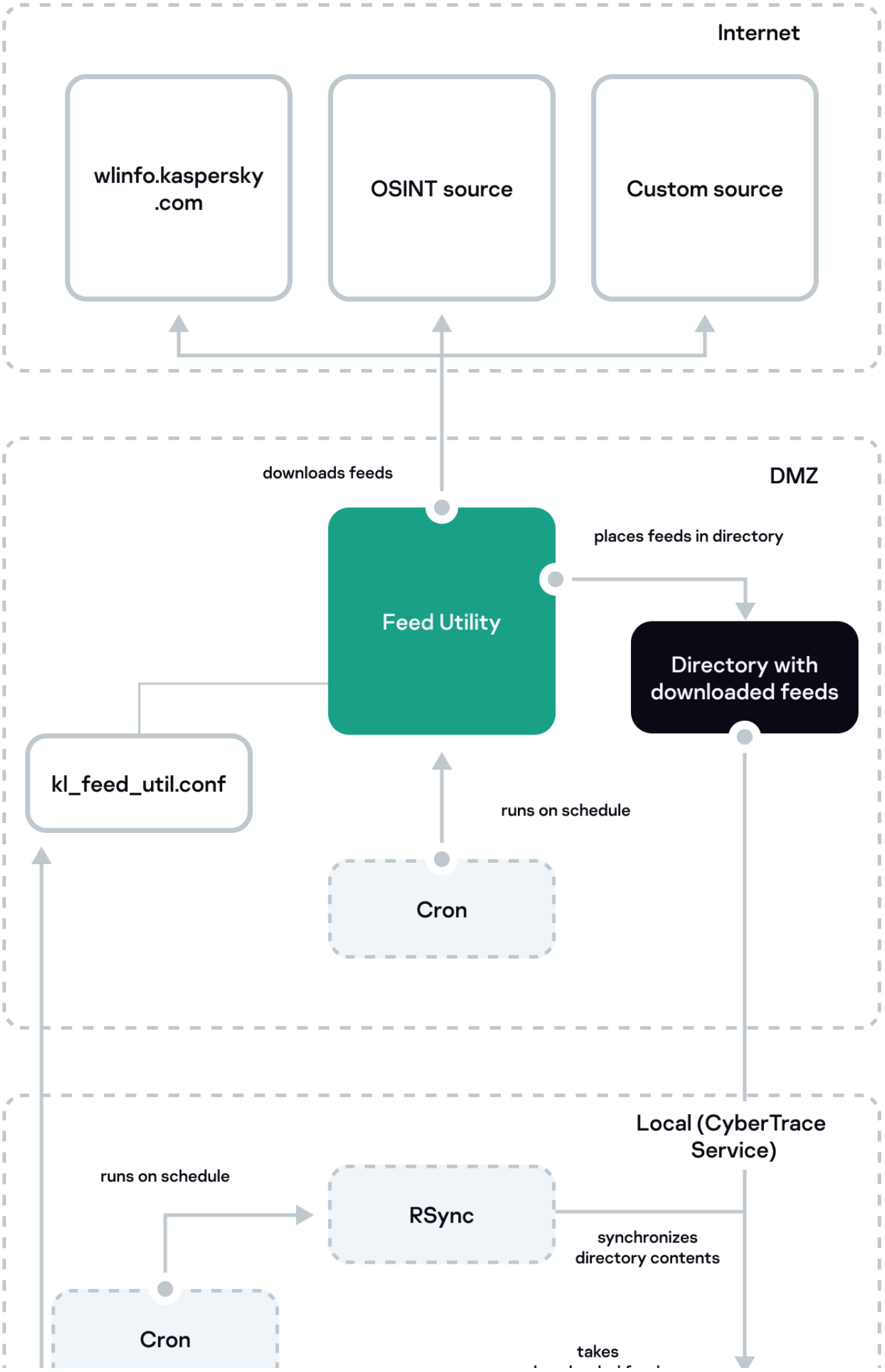
Раздельная установка Kaspersky CyberTrace Service и Feed Utility (Windows, сценарий DMZ)

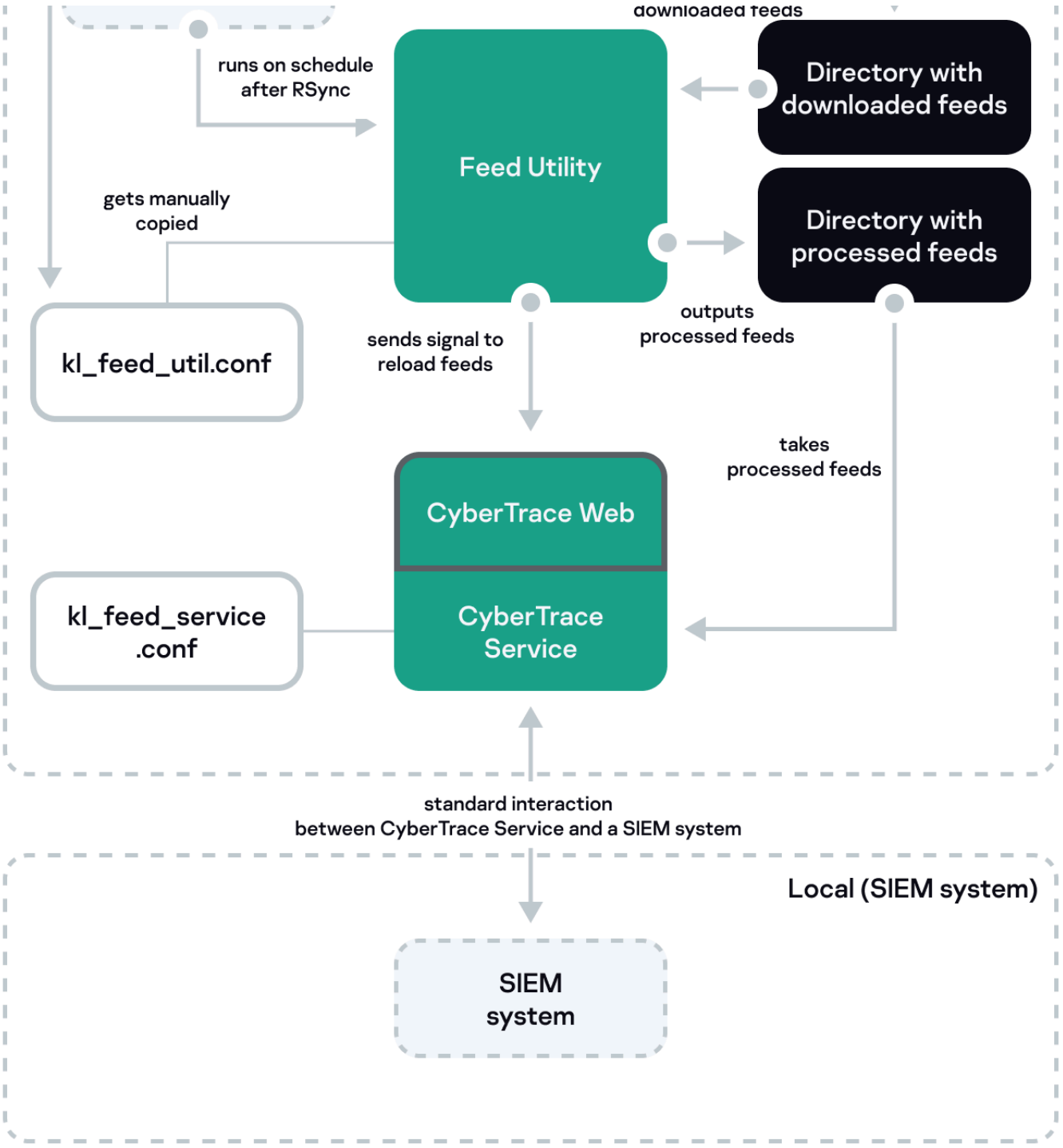
Kaspersky CyberTrace Service и Feed Utility можно установить на разные хосты. Это позволяет изолировать от интернета хост, на котором данные о событиях сопоставляются с потоками данных об угрозах.

Каталог `dmz` из комплекта поставки Kaspersky CyberTrace не следует удалять, даже если Kaspersky CyberTrace Service и Feed Utility не планируется использовать на разных хостах.

Работа Kaspersky CyberTrace Service и Feed Utility работают в демилитаризованной зоне (DMZ)

На следующей схеме показана работа как Kaspersky CyberTrace Service и Feed Utility в демилитаризованной зоне.


Internet
wlinfo.kaspersky .com
OSINT source
Custom source
downloads feeds
DMZ
places feeds in directory
Feed Utility
Directory with downloaded feeds
kl_feed_util.conf
runs on schedule
Cron
Local (CyberTrace Service)
runs on schedule
RSync
synchronizes directory contents
Cron
takes



Рабочий процесс при установке Kaspersky CyberTrace Service и Feed Utility на разных хостах

Ограничения Kaspersky CyberTrace при работе в изолированной среде

Поскольку Kaspersky CyberTrace будет работать на хосте без прямого доступа в интернет, будут иметь место следующие ограничения работы Kaspersky CyberTrace:

- Отсутствует возможность обогащения графов из сторонних источников на локальном хосте Kaspersky CyberTrace.
- Для добавления потоков данных настройки Kaspersky CyberTrace необходимо перенести с локального хоста на хост DMZ, изменить их там, а затем перенести обратно на локальный хост. Дополнительную информацию см. в разделе «Изменение параметров потоков данных об угрозах после установки Kaspersky CyberTrace Service и Feed Utility на разных хостах».

Установка Kaspersky CyberTrace Service и Feed Utility (сценарий DMZ)

Следующая процедура описывает порядок настройки хоста DMZ и локального хоста для установки Kaspersky CyberTrace Service на одном хосте (в этом разделе называется «локальным») и Feed Utility на другом хосте (в этом разделе называется «DMZ»).

Настройка хоста DMZ

Порядок настройки хоста DMZ:

1. Установите Kaspersky CyberTrace на хосте DMZ для удобства настройки потоков данных, которые предполагается загружать в Kaspersky CyberTrace в изолированной среде.

2. В мастере первоначальной настройки задайте необходимые параметры SIEM (имя, данные подключения).

   Эти настройки в дальнейшем будут использоваться для локального хоста.

   Также добавьте сертификат в формате PEM для настройки потоков данных об угрозах «Лаборатории Касперского», которые будут использоваться. Добавлять лицензионный ключ Kaspersky CyberTrace на хост DMZ не требуется, поскольку редакция Community позволяет настраивать все поддерживаемые типы потоков данных об угрозах. Добавление лицензионного ключа на локальном хосте является обязательным.

3. При необходимости добавьте или дополнительно настройте потоки данных об угрозах на странице **Параметры → Потоки данных** после настройки параметров в мастере первоначальной настройки.

   > Убедитесь, что потоки данных настроены правильно, для этого запустите обновление потоков данных в Kaspersky CyberTrace хотя бы один раз.

4. Экспортируйте параметры из Kaspersky CyberTrace, для этого нажмите кнопку **Экспортировать конфигурационный файл** на странице **Параметры → Служба**.

   Если пользовательские потоки данных об угрозах были ранее настроены в Kaspersky CyberTrace, также сохраните файл `httpsrv\etc\custom_feed_list.conf` для дальнейшего использования.

5. Скопируйте каталог `%service_dir%\dmz` куда-либо кроме каталога `%service_dir%` (например, в каталог `C:\Users\%UserName%`).

   В дальнейшем путь к этому каталогу будет обозначаться как `%dmz_fu%`.

6. Удалите Kaspersky CyberTrace.

   > Если потребуется добавить новые потоки данных, Kaspersky CyberTrace можно будет снова установить на хосте DMZ.

7. Перенесите разделы `Settings → Feeds` и `Settings → ProxySettings` из экспортированного файла `kl_feed_util.conf` (см. шаг 4) в файл `%dmz_fu%\kl_feed_util.conf` (если раздел уже присутствует в целевом конфигурационном файле, замените этот раздел новыми данными).

   > Не удаляйте экземпляр файла `kl_feed_util.conf`, экспортированный из Kaspersky CyberTrace, а также файл `kl_feed_service.conf`. Эти файлы будут использоваться на локальном хосте.

8. Укажите значение `accepted` в теге `Settings` > `EULA` в файле `%dmz_fu%\kl_feed_util.conf`.

9. Укажите `<WorkDir>tmp_download</WorkDir>` в разделе `Settings/WorkDir` файла `%dmz_fu%\kl_feed_util.conf`.

10. Добавьте файл `%dmz_fu%\cron_dmz.cmd` в список задач schtasks.

    Скрипт `cron_dmz.cmd` позволяет загружать потоки данных об угрозах на хост DMZ.

    В приведенном ниже примере скрипт `cron_dmz.cmd` выполняется один раз в 30 минут:

    ```
    schtasks /create /tn KasperskyFeedServiceUpdate /ru system /f /tr
    "\"%dmz_fu%\cron_dmz.cmd\"" /sc minute /mo 30
    ```

    Можно задать собственное расписание запуска скрипта.

Настройка локального хоста

Порядок настройки локального хоста:

1. Проверьте доступность хоста DMZ с локального хоста с помощью утилиты RSync (для этого выполните шаги из раздела «Синхронизация каталогов, содержащих потоки данных об угрозах»).

2. На локальном хосте установите Kaspersky CyberTrace той же версии, что была ранее установлена на хосте DMZ.

3. После установки остановите Kaspersky CyberTrace командой `sc stop cybertrace`.

4. Удалите файл `%service_dir%\bin\.need_run_wizard`.

   Это действие отключает мастер первоначальной настройки, поскольку настройка уже была выполнена на хосте DMZ.

5. Замените файлы `%service_dir%\bin\kl_feed_util.conf` и `%service_dir%\bin\kl_feed_service.conf` файлами, полученными на шаге 4 раздела «Настройка хоста DMZ».

   Если пользовательские потоки данных об угрозах ранее были настроены в Kaspersky CyberTrace, также замените файл `httpsrv\etc\custom_feed_list.conf` (или добавьте его, если он отсутствовал).

6. Откройте файл `%service_dir%\bin\kl_feed_util.conf` и задайте следующие параметры:

   - `<NotifyKTFS path="../bin">true</NotifyKTFS>`
   - `<WorkDir>output</WorkDir>`
   - `<FeedsDir>../feeds/download</FeedsDir>`

7. Выполните следующую настройку в файле `%service_dir%\bin\kl_feed_service.conf`:

   - Задайте настройки в следующих разделах:
     - `Configuration` → `InputSettings` → `ConnectionString`
     - `Configuration` > `ServiceSettings` > `HTTPServer` > `ConnectionString`
     - `Configuration` > `ServiceSettings` > `HTTPServer` > `ResourcesIP`

- Задайте значение `0` для атрибута `update_frequency`.

  Эта пользовательская настройка применяется, поскольку файлы потоков данных, загруженные на хост DMZ, будут периодически синхронизироваться с помощью Schtasks, а не Kaspersky CyberTrace.

8. (Рекомендуется) Переименуйте файл `%service_dir%\dmz\feeds.pem` в `feeds.pem.0`, чтобы исключить некорректное обновление потоков данных об угрозах при нажатии кнопки (**Обновить сейчас**).

9. Откройте файл `%service_dir%\scripts\cron_cybertrace.cmd` и задайте следующие параметры:

   - `RSYNC_USER` (имя пользователя на хоста DMZ для авторизации).
   - `RSYNC_HOST` (имя хоста/IP-адрес хоста DMZ).
   - `PATH_TO_FEEDS` (путь к каталогу `%dmz_fu%/download` на хосте DMZ).
   - `DOWNLOAD_DIR` ("output").
   - `SSH_KEY` (убедитесь, что указан тот же путь к файлу ключа RSA, как и на шаге 1 раздела «Синхронизация каталогов, содержащих потоки данных об угрозах»).

10. Добавьте `%service_dir%\scripts\cron_cybertrace.cmd` в список задач cron.

    Скрипт `cron_cybertrace.cmd` запускает синхронизацию файлов потоков данных об угрозах с хоста DMZ. В следующем примере показано, что файл cron_dmz.cmd запускается один раз в 30 минут:

    ```
    schtasks /create /tn KasperskyFeedServiceUpdate /ru %user% /rp %password% /f /tr
    "%service_dir%\scripts\cron_cybertrace.cmd" /sc minute /mo 30
    ```

    Можно установить собственное расписание синхронизации.

11. Запустите Kaspersky CyberTrace.

    Выполните команду `sc start cybertrace`.

12. Откройте веб-интерфейс Kaspersky CyberTrace в браузере (введите данные, указанные на шаге 7, в разделе `Configuration` > `GUISettings` > `HTTPServer` > `ConnectionString`).

13. Убедитесь, что настройки потоков данных об угрозах на странице **Параметры** → **Потоки данных** похожи на соответствующие настройки на хосте DMZ.

14. На странице **Параметры** → **Потоки данных** задайте значение **Никогда** для параметра **Частота обновления по умолчанию**.

15. На странице **Параметры** → **Лицензирование** добавьте лицензионный ключ.

16. Настройте прочие параметры, не связанные с обновлением потоков данных об угрозах.

Изменение параметров потоков данных об угрозах после установки Kaspersky CyberTrace Service и Feed Utility на разных хостах (сценарий DMZ)

Поскольку хост DMZ предназначен только для загрузки потоков данных, следующие настройки можно задать для ранее включенных потоков данных в Kaspersky CyberTrace на локальном хосте. Можно изменить следующие параметры потоков данных об угрозах:

- Значение `confidence` для потока данных об угрозах (кроме потоков данных об угрозах «Лаборатории Касперского»)
- Ограничение на количество обрабатываемых записей потока данных об угрозах

- Срок хранения (кроме потоков данных об угрозах «Лаборатории Касперского»)
- Доступные поля для потока данных об угрозах
- Правила фильтрации
- Поля контекста

Также можно отключить любой поток данных об угрозах, который ранее был включен (в этом случае отключенные потоки данных об угрозах продолжат загружаться на хост DMZ и передаваться на локальный хост, пока они не будут отключены в файле `%dmz_fu%/kl_feed_util.conf`).

Параметры прокси-сервера можно настроить непосредственно в файле `%dmz_fu%\kl_feed_util.conf` на хосте DMZ.

При необходимости можно добавить новый поток данных об угрозах, как описано ниже.

Если какой-либо поток данных об угрозах был ранее отключен на локальном хосте, загрузка данных об угрозах на хосте DMZ прекратится после выполнения следующих действий.

Чтобы добавить новый поток данных, выполните следующие действия:

1. На локальном хосте:
   a. Экспортируйте текущие настройки из Kaspersky CyberTrace, для этого нажмите кнопку **Экспортировать конфигурационный файл** на странице **Параметры → Служба**.

      Если пользовательские потоки данных об угрозах были ранее настроены в Kaspersky CyberTrace, также сохраните файл `httpsrv\etc\custom_feed_list.conf` для дальнейшего использования.

   b. Остановите службу Kaspersky CyberTrace.

      Выполните команду `sc stop cybertrace`.

2. На хосте DMZ:
   a. Установите ту же версию Kaspersky CyberTrace, что и на локальном хосте.

      Если во время первоначальной настройки Kaspersky CyberTrace на узле DMZ не удалялся, пропустите этот шаг.

   b. Остановите службу Kaspersky CyberTrace.

      Выполните команду `sc stop cybertrace`.

   c. Удалите файл `%service_dir%/bin/.need_run_wizard`.

      Если во время первоначальной настройки Kaspersky CyberTrace на узле DMZ не удалялся, пропустите этот шаг.

d. Замените файлы `%service_dir%\bin\kl_feed_service.conf` и `%service_dir%\bin\kl_feed_util.conf` файлами, экспортированными с локального хоста на шаге 1 выше.

Если пользовательские потоки данных об угрозах ранее были настроены в Kaspersky CyberTrace, также замените файл `httpsrv\etc\custom_feed_list.conf` (или добавьте его, если он отсутствовал).

> Укажите правильную строку `Configuration` > `ServiceSettings` > `HTTPServer` > `ConnectionString`, чтобы открыть веб-интерфейс Kaspersky CyberTrace в браузере.

e. Запустите службу Kaspersky CyberTrace.

Выполните команду `sc start cybertrace`.

f. Добавьте и настройте новые потоки данных об угрозах с помощью веб-интерфейса Kaspersky CyberTrace по адресу, указанному в параметре `Configuration` > `ServiceSettings` > `HTTPServer` > `ConnectionString` в файле `%service_dir%\bin\kl_feed_service.conf`

> Убедитесь, что потоки данных об угрозах настроены правильно, для этого запустите обновление потоков данных об угрозах в Kaspersky CyberTrace хотя бы один раз.

g. Экспортируйте обновленные настройки из Kaspersky CyberTrace, для этого нажмите кнопку **Экспортировать конфигурационный файл** на странице **Параметры → Служба**.

Если пользовательские потоки данных об угрозах были ранее настроены в Kaspersky CyberTrace, также сохраните файл `httpsrv\etc\custom_feed_list.conf` для дальнейшего использования.

h. Удалите Kaspersky CyberTrace.

i. Переместите (с заменой) разделы `Settings/Feeds` и `Settings/ProxySettings` из экспортированного файла `kl_feed_util.conf` в файл `%dmz_fu%\kl_feed_util.conf`.

> Не удаляйте экземпляр файла `kl_feed_util.conf`, экспортированный из Kaspersky CyberTrace, а также файл `kl_feed_service.conf`. Эти файлы будут использоваться на локальном хосте.

3. На локальном хосте:

a. Замените файлы `%service_dir%\bin\kl_feed_service.conf` и `%service_dir%\bin\kl_feed_util.conf` файлами, экспортированными с хоста DMZ.

Если пользовательские потоки данных об угрозах ранее были настроены в Kaspersky CyberTrace, также замените файл `httpsrv\etc\custom_feed_list.conf` (или добавьте его, если он отсутствовал).

> Укажите правильную строку `Configuration` > `ServiceSettings` > `HTTPServer` > `ConnectionString`, чтобы открыть веб-интерфейс Kaspersky CyberTrace в браузере.

b. Запустите службу Kaspersky CyberTrace.

Выполните команду `sc start cybertrace`.

c. Откройте веб-интерфейс Kaspersky CyberTrace по адресу, указанному в параметре `Configuration > ServiceSettings > HTTPServer > ConnectionString`, и убедитесь, что страница **Параметры → Потоки данных** содержит только что добавленный поток данных и его настройки аналогичны настройкам на хосте DMZ. Также убедитесь, что все остальные потоки данных об угрозах настроены правильно.

d. На странице **Параметры → Потоки данных** задайте значение **Никогда** для параметра **Частота обновления по умолчанию**.

Синхронизация каталогов, содержащих потоки данных об угрозах (сценарий DMZ)

Для синхронизации потоков данных об угрозах на локальном хосте и на хосте DMZ можно использовать утилиту RSync. На хосте с ОС Windows утилиту RSync можно запустить с помощью Cygwin.

> Все приведенные ниже команды Linux на хостах с Windows следует запускать с помощью Cygwin.

Чтобы установить утилиту RSync на хост с ОС Windows:

1. Установите набор пакетов по умолчанию из дистрибутива Cygwin.
2. Установите следующие утилиты: OpenSSH, OpenSSL и RSync.
3. На хосте DMZ настройте компоненты OpenSSH следующим образом:

   a. Выполните следующую команду как root:

   ```
   ssh-host-config
   ```

   На все вопросы можно ответить `Yes`. Смысл операции в том, чтобы запустить демон sshd как службу.

   b. Выполните следующую команду:

   ```
   net start sygsshd
   ```

Демон sshd автоматически запустится.

Чтобы настроить синхронизацию на локальном хосте, выполните следующие действия:

1. Создайте закрытый ключ и соответствующий открытый ключ.

   Для этого выполните на локальном хосте следующую команду:

   ```
   ssh-keygen -t rsa -q -N '' -f /home/<пользователь>/.ssh/dmz_rsa_key
   ```

   Укажите логин пользователя вместо `<user>`. Ключи будут созданы без пароля.

2. Скопируйте открытый ключ с локального хоста на хост DMZ, для этого выполните следующую команду:

   ```
   ssh-copy-id -i /home/<пользователь>/.ssh/dmz_rsa_key <пользователь_DMZ>@<хост_DMZ>
   ```

   После запуска этой команды предлагается ввести пароль для `<DMZ_user>@<DMZ_host>`.

3. Проверьте синхронизацию содержимого каталогов, содержащих потоки данных об угрозах, для этого выполните следующую команду на локальном хосте:

   ```
   rsync -a --delete-before --delay-updates -e "ssh -i
   /home/<пользователь>/.ssh/dmz_rsa_key" <пользователь_DMZ>@<хост_DMZ>:/<Path_to_feeds>/
   /<Path_to_feeds_on_Local>/
   ```

   В этой команде `<Path_to_feeds_on_Local>` — это путь к папке, содержащей потоки данных об угрозах на локальном хосте (а именно, `%service_dir%/feeds`), а `<Path_to_feeds>` — это путь к папке, в которой хранятся обновленные потоки данных об угрозах на хосте DMZ.

Чтобы проверка синхронизации была пройдена, содержимое папки `<Path_to_feeds_on_Local>` на локальном хосте должно совпадать с содержимым папки `<Path_to_feeds>` на хосте DMZ.

При тестировании Rsync с помощью Cygwin могут возникнуть проблемы, связанные с символами пробела в пути, поэтому рекомендуется принять следующие меры:

1. Путь к каталогу на хосте DMZ следует указывать в кавычках и экранировать пробел ("\ ").
2. Следует экранировать пробел ("\ ") в пути к каталогу на локальном хосте.

Чтобы перейти к каталогу на диске C:\ с помощью Cygwin, необходимо указать путь `/cygdrive/c/`, а далее обычный путь (/cygdrive/c/Users/...).

Обновление Kaspersky CyberTrace с предыдущей версии (сценарий DMZ)

Чтобы обновить Kaspersky CyberTrace и Feed Utility до более новых версий, выполните следующие действия:

1. Обновите Kaspersky CyberTrace на локальном хосте, как описано в разделе Автоматическое обновление в ОС Windows.
2. Переместите файл `kl_feed_util.exe` из каталога `%service_dir%\dmz` на локальном хосте в `%dmz_fu%\kl_feed_util` на хосте DMZ.

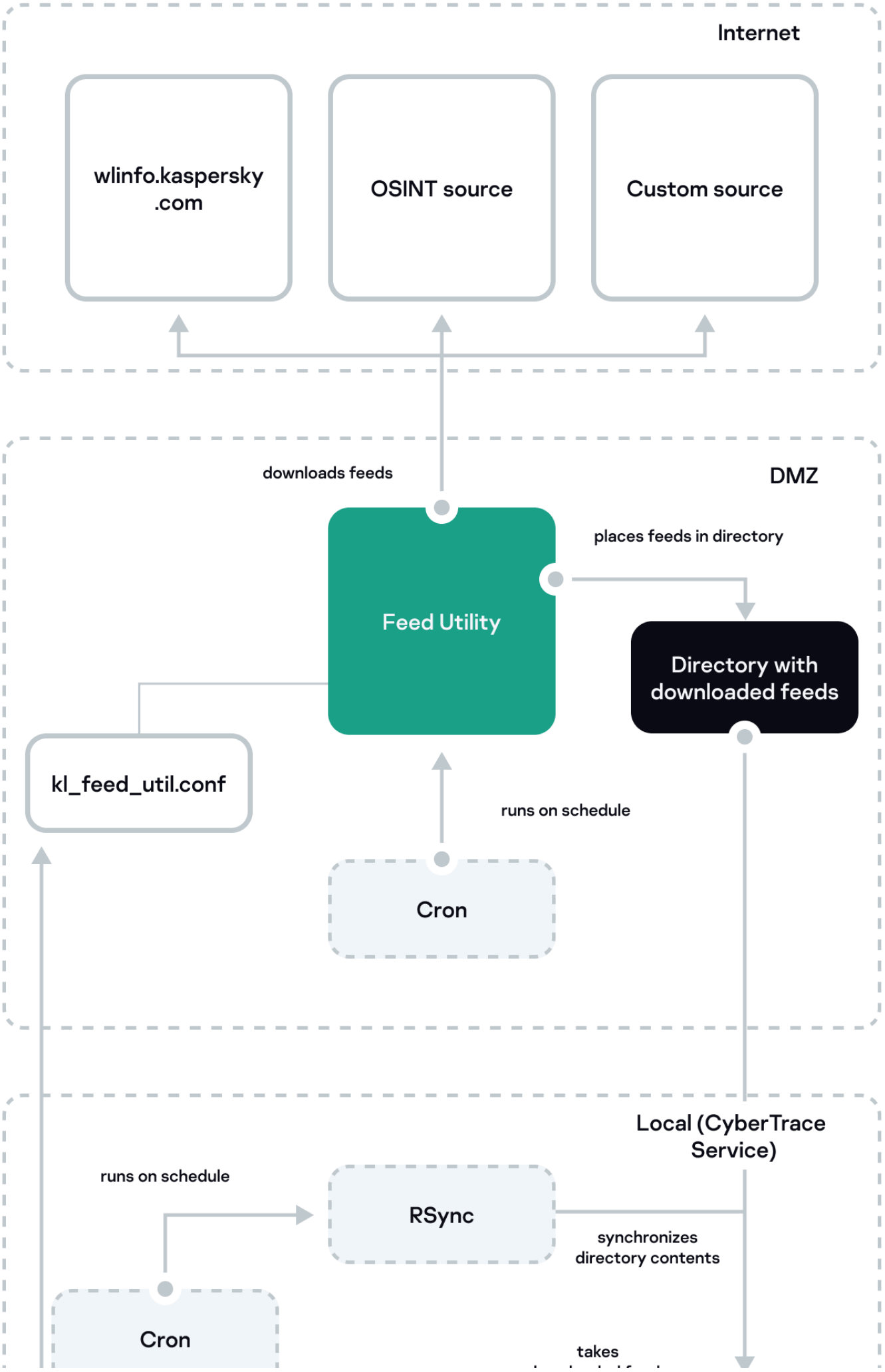
Раздельная установка Kaspersky CyberTrace Service и Feed Utility (Linux, сценарий DMZ)

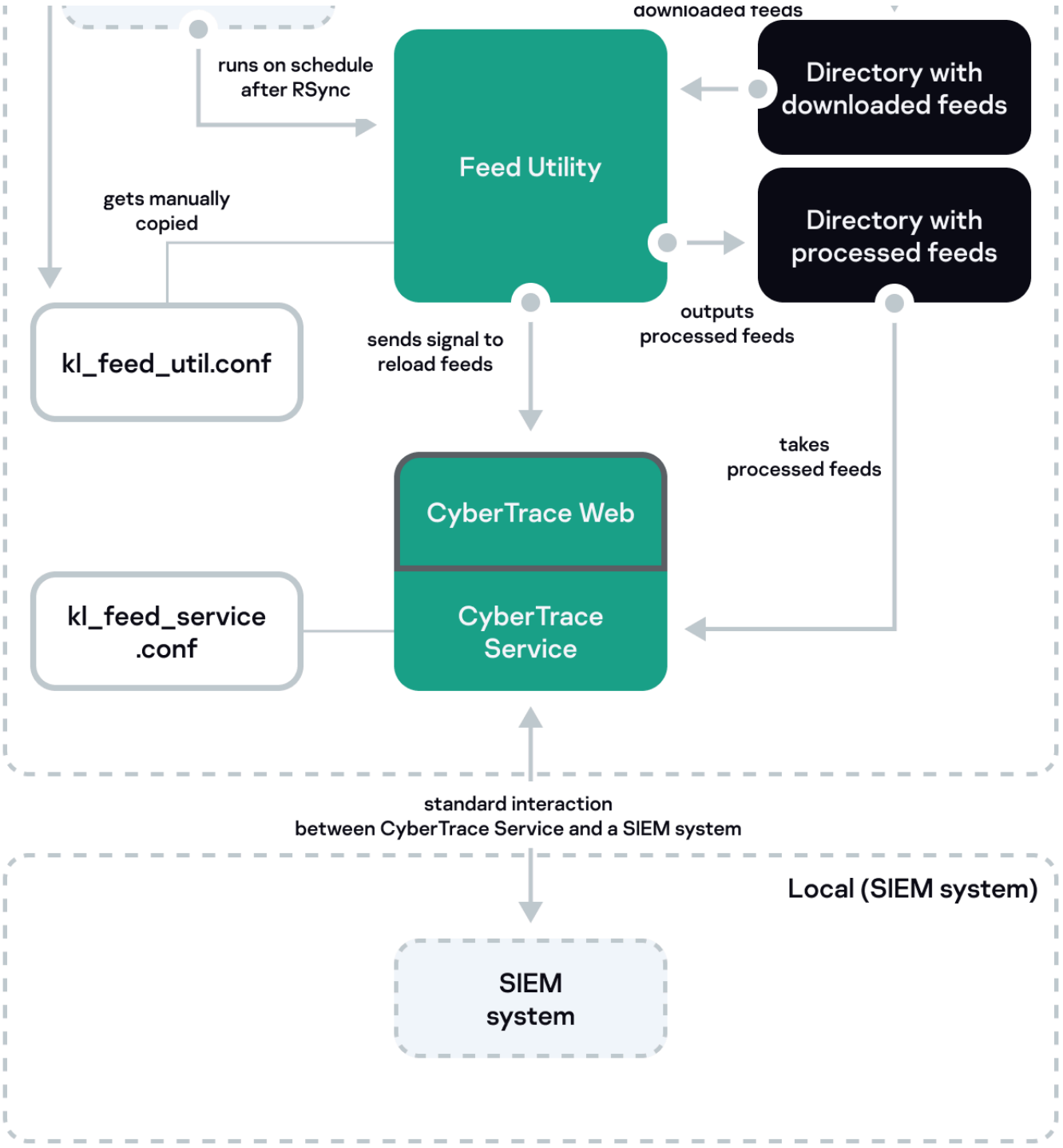
Kaspersky CyberTrace Service и Feed Utility можно установить на разные хосты. Это позволяет изолировать от интернета хост, на котором данные о событиях сопоставляются с потоками данных об угрозах.

Каталог `dmz` из комплекта поставки Kaspersky CyberTrace не следует удалять, даже если Kaspersky CyberTrace Service и Feed Utility не планируется использовать на разных хостах.

Работа Kaspersky CyberTrace Service и Feed Utility работают в демилитаризованной зоне (DMZ)

На следующей схеме показана работа как Kaspersky CyberTrace Service и Feed Utility в демилитаризованной зоне.


Internet
wlinfo.kaspersky .com
OSINT source
Custom source
downloads feeds
DMZ
places feeds in directory
Feed Utility
Directory with downloaded feeds
kl_feed_util.conf
runs on schedule
Cron
Local (CyberTrace Service)
runs on schedule
RSync
synchronizes directory contents
Cron
takes



Рабочий процесс при установке Kaspersky CyberTrace Service и Feed Utility на разных хостах

Ограничения Kaspersky CyberTrace при работе в изолированной среде

Поскольку Kaspersky CyberTrace будет работать на хосте без прямого доступа в интернет, будут иметь место следующие ограничения работы Kaspersky CyberTrace:

- Отсутствует возможность обогащения графов из сторонних источников на локальном хосте Kaspersky CyberTrace.
- Для добавления потоков данных настройки Kaspersky CyberTrace необходимо перенести с локального хоста на хост DMZ, изменить их там, а затем перенести обратно на локальный хост. Дополнительную информацию см. в разделе «Изменение параметров потоков данных об угрозах после установки Kaspersky CyberTrace Service и Feed Utility на разных хостах».

Установка Kaspersky CyberTrace Service и Feed Utility (сценарий DMZ)

Следующая процедура описывает порядок настройки хоста DMZ и локального хоста для установки Kaspersky CyberTrace Service на одном хосте (в этом разделе называется «локальным») и Feed Utility на другом хосте (в этом разделе называется «DMZ»).

Настройка хоста DMZ

Порядок настройки хоста DMZ:

1. Установите Kaspersky CyberTrace на хосте DMZ для удобства настройки потоков данных, которые предполагается загружать в Kaspersky CyberTrace в изолированной среде.

2. В мастере первоначальной настройки задайте необходимые параметры SIEM (имя, данные подключения).

   Эти настройки будут использоваться для локального хоста.

   Также добавьте сертификат в формате PEM для настройки потоков данных об угрозах «Лаборатории Касперского», которые будут использоваться. Добавлять лицензионный ключ Kaspersky CyberTrace на хост DMZ не требуется, поскольку редакция Community позволяет настраивать все поддерживаемые типы потоков данных об угрозах. Добавление лицензионного ключа на локальном хосте является обязательным.

3. При необходимости добавьте или дополнительно настройте потоки данных об угрозах на странице **Параметры → Потоки данных** после настройки параметров в мастере первоначальной настройки.

   > Убедитесь, что потоки данных об угрозах настроены правильно, для этого запустите обновление потоков данных об угрозах в Kaspersky CyberTrace хотя бы один раз.

4. Экспортируйте параметры из Kaspersky CyberTrace, для этого нажмите кнопку **Экспортировать конфигурационный файл** на странице **Параметры → Служба**.

   Если пользовательские потоки данных об угрозах были ранее настроены в Kaspersky CyberTrace, также сохраните файл `httpsrv/etc/custom_feed_list.conf` для дальнейшего использования.

5. Скопируйте каталог `%service_dir%\dmz` куда-либо кроме каталога `%service_dir%` (например, в каталог `/opt` или `/usr/local/etc`).

   В дальнейшем путь к этому каталогу будет обозначаться как `%dmz_fu%`.

6. Удалите Kaspersky CyberTrace.

   > Если потребуется добавить новые потоки данных, Kaspersky CyberTrace можно будет снова установить на хосте DMZ.

7. Перенесите разделы `Settings → Feeds` и `Settings → ProxySettings` из экспортированного файла `kl_feed_util.conf` (см. шаг 4) в файл `%dmz_fu%/kl_feed_util.conf` (если раздел уже присутствует в целевом конфигурационном файле, замените этот раздел новыми данными).

   > Не удаляйте экземпляр файла `kl_feed_util.conf`, экспортированный из Kaspersky CyberTrace, а также файл `kl_feed_service.conf`. Эти файлы будут использоваться на локальном хосте.

8. Укажите значение `accepted` в теге `Settings → EULA` в файле `%dmz_fu%/kl_feed_util.conf`.

9. Укажите `<WorkDir>tmp_download</WorkDir>` в разделе `Settings/WorkDir` файла `%dmz_fu%/kl_feed_util.conf`.

10. Добавьте `%dmz_fu%/cron_dmz.sh` в список задач cron.

    Скрипт `cron_dmz.sh` позволяет загружать потоки данных об угрозах на хост DMZ.

    Например, в конфигурационном файле cron укажите следующую строку:

    `*/30 * * * * %dmz_fu%/cron_dmz.sh`

    В приведенном выше примере скрипт `cron_dmz.sh` выполняется один раз в 30 минут. Можно задать собственное расписание запуска скрипта.

    > Убедитесь, что у пользователя cron есть права на запуск файла `%dmz_fu%/cron_dmz.sh`.

Настройка локального хоста

Порядок настройки локального хоста:

1. Проверьте доступность узла DMZ для локального узла с помощью утилиты RSync (для этого выполните шаги из раздела «Синхронизация каталогов, содержащих потоки данных об угрозах»).

2. На локальном хосте установите Kaspersky CyberTrace той же версии, что была ранее установлена на хосте DMZ.

3. После установки остановите Kaspersky CyberTrace командой `systemctl stop cybertrace.service`.

4. Удалите файл `%service_dir%/bin/.need_run_wizard`.

   Это действие отключает мастер первоначальной настройки, поскольку настройка уже была выполнена на хосте DMZ.

5. Замените файлы `%service_dir%/etc/kl_feed_util.conf` и `%service_dir%/etc/kl_feed_service.conf` файлами, полученными на шаге 4 раздела «Настройка хоста DMZ».

   Если пользовательские потоки данных об угрозах ранее были настроены в Kaspersky CyberTrace, замените файл `httpsrv/etc/custom_feed_list.conf` (или добавьте его, если он отсутствовал).

6. Откройте файл `%service_dir%/etc/kl_feed_util.conf` и задайте следующие параметры:

   - `<NotifyKTFS path="../bin">true</NotifyKTFS>`
   - `<WorkDir>output</WorkDir>`
   - `<FeedsDir>../feeds/download</FeedsDir>`

7. Выполните следующую настройку в файле `%service_dir%/etc/kl_feed_service.conf`:

   - Задайте настройки в следующих разделах:
     - `Configuration` → `InputSettings` → `ConnectionString`
     - `Configuration` → `GUISettings` → `HTTPServer` → `ConnectionString`
     - `Configuration` → `GUISettings` → `HTTPServer` → `ResourcesIP`
   - Задайте `значение 0` в атрибуте `update_frequency`.

     Эта пользовательская настройка применяется, поскольку файлы потоков данных, загруженные на хост DMZ, будут периодически синхронизироваться с помощью cron, а не Kaspersky CyberTrace.

8. (Рекомендуется) Переименуйте файл `%service_dir%/dmz/feeds.pem` в `feeds.pem.0`, чтобы исключить некорректное обновление потоков данных об угрозах при нажатии кнопки (**Обновить сейчас**).

9. Откройте файл `%service_dir%/scripts/cron_cybertrace.sh` и задайте следующие параметры:

   - `RSYNC_USER` (имя пользователя на хоста DMZ для авторизации).
   - `RSYNC_HOST` (имя хоста/IP-адрес хоста DMZ).
   - `PATH_TO_FEEDS` (путь к каталогу `%dmz_fu%/download` на хосте DMZ).
   - `DOWNLOAD_DIR` ("output").
   - `SSH_KEY` (убедитесь, что указан тот же путь к файлу ключа RSA, как и на шаге 1 раздела «Синхронизация каталогов, содержащих потоки данных об угрозах»).

10. Добавьте `%service_dir%/scripts/cron_cybertrace.sh` в список задач cron.

    Скрипт `cron_cybertrace.sh` запускает синхронизацию файлов потоков данных об угрозах с хоста DMZ. В приведенном ниже примере файл `cron_cybertrace.sh` запускается один раз в 30 минут, причем запуск осуществляется с пятиминутной задержкой относительно скрипта `cron_dmz.sh` на узле DMZ:

    ```
    5-59/30 * * * * /opt/kaspersky/ktfs/scripts/cron_cybertrace.sh
    ```

    Можно задать собственное расписание запуска скрипта.

    > Убедитесь, что у пользователя cron есть права на запуск файла `%service_dir%/scripts/cron_cybertrace.sh`.

11. Запустите Kaspersky CyberTrace.

    Выполните команду `systemctl start cybertrace.service`.

12. Откройте веб-интерфейс Kaspersky CyberTrace в браузере (введите данные, указанные на шаге 7, в разделе `Configuration>GUISettings>HTTPServer>ConnectionString`).

13. Убедитесь, что настройки потоков данных об угрозах на странице **Параметры** → **Потоки данных** похожи на соответствующие настройки на хосте DMZ.

14. На странице **Параметры** → **Потоки данных** задайте значение **Никогда** для параметра **Частота обновления по умолчанию**.

15. На странице **Параметры** → **Лицензирование** добавьте лицензионный ключ.

16. Настройте прочие параметры, не связанные с обновлением потоков данных об угрозах.

Изменение параметров потоков данных об угрозах после установки Kaspersky CyberTrace Service и Feed Utility на разных хостах (сценарий DMZ)

Поскольку хост DMZ предназначен только для загрузки потоков данных об угрозах, следующие настройки можно задать для ранее включенных потоков данных об угрозах в Kaspersky CyberTrace на локальном хосте. Можно изменить следующие параметры потоков данных об угрозах:

- Значение `confidence` для потока данных об угрозах (кроме потоков данных об угрозах «Лаборатории Касперского»)
- Ограничение на количество обрабатываемых записей потока данных об угрозах
- Срок хранения (кроме потоков данных об угрозах «Лаборатории Касперского»)
- Доступные поля для потока данных об угрозах
- Правила фильтрации
- Поля контекста

Также можно отключить любой поток данных об угрозах, который ранее был включен (в этом случае отключенные потоки данных об угрозах продолжат загружаться на хост DMZ и передаваться на локальный хост, пока они не будут отключены в файле `%dmz_fu%/kl_feed_util.conf`).

> Параметры прокси-сервера можно настроить непосредственно в файле `%dmz_fu%/kl_feed_util.conf` на хосте DMZ.

При необходимости можно добавить новый поток данных об угрозах, как описано ниже.

> Если какой-либо поток данных об угрозах был ранее отключен на локальном хосте, загрузка данных об угрозах на хосте DMZ прекратится после выполнения следующих действий.

Чтобы добавить новый поток данных, выполните следующие действия:

1. На локальном хосте:

   a. Экспортируйте текущие настройки из Kaspersky CyberTrace, для этого нажмите кнопку **Экспортировать конфигурационный файл** на странице **Параметры → Служба**.

   Если пользовательские потоки данных об угрозах были ранее настроены в Kaspersky CyberTrace, также сохраните файл `httpsrv/etc/custom_feed_list.conf` для дальнейшего использования.

   b. Остановите службу Kaspersky CyberTrace.

   Выполните команду `systemctl stop cybertrace.service`.

2. На хосте DMZ:

a. Установите ту же версию Kaspersky CyberTrace, что и на локальном хосте.

> Если во время первоначальной настройки Kaspersky CyberTrace на узле DMZ не удалялся, пропустите этот шаг.

b. Остановите службу Kaspersky CyberTrace.

Выполните команду `systemctl stop cybertrace.service`.

c. Удалите файл `%service_dir%/bin/.need_run_wizard`.

> Если во время первоначальной настройки Kaspersky CyberTrace на узле DMZ не удалялся, пропустите этот шаг.

d. Замените файлы `%service_dir%/etc/kl_feed_service.conf` и `%service_dir%/etc/kl_feed_util.conf` файлами, экспортированными с локального хоста на шаге 1 выше.

Если пользовательские потоки данных об угрозах ранее были настроены в Kaspersky CyberTrace, также замените файл `httpsrv/etc/custom_feed_list.conf` (или добавьте его, если он отсутствовал).

> Укажите правильную строку `Configuration → GUISettings → HTTPServer → ConnectionString`, чтобы открыть веб-интерфейс Kaspersky CyberTrace в браузере.

e. Запустите службу Kaspersky CyberTrace.

Выполните команду `systemctl start cybertrace.service`.

f. Добавьте и настройте новые потоки данных с помощью веб-интерфейса Kaspersky CyberTrace Web по адресу, указанному в параметре `Configuration/GUISettings/HTTPServer/ConnectionString` в файле `%service_dir%/etc/kl_feed_service.conf`.

> Убедитесь, что поток данных настроен правильно, для этого запустите обновление потоков данных в Kaspersky CyberTrace хотя бы один раз.

g. Экспортируйте обновленные настройки из Kaspersky CyberTrace, для этого нажмите кнопку **Экспортировать конфигурационный файл** на странице **Параметры → Служба**.

Если пользовательские потоки данных об угрозах были ранее настроены в Kaspersky CyberTrace, также сохраните файл `httpsrv/etc/custom_feed_list.conf` для дальнейшего использования.

h. Удалите Kaspersky CyberTrace.

i. Переместите (с заменой) разделы `Settings>Feeds` and `Settings>ProxySettings` из экспортированного файла `kl_feed_util.conf` в файл `%dmz_fu%/kl_feed_util.conf`.

> Не удаляйте экземпляр файла `kl_feed_util.conf`, экспортированный из Kaspersky CyberTrace, а также файл `kl_feed_service.conf`. Эти файлы также будут использоваться на локальном хосте.

3. На локальном хосте:

   a. Замените файлы `%service_dir%/etc/kl_feed_service.conf` и `%service_dir%/etc/kl_feed_util.conf` файлами, экспортированными с хоста DMZ.

      Если пользовательские потоки данных об угрозах ранее были настроены в Kaspersky CyberTrace, также замените файл `httpsrv/etc/custom_feed_list.conf` (или добавьте его, если он отсутствовал).

      > Укажите правильную строку `Configuration → GUISettings → HTTPServer → ConnectionString`, чтобы открыть веб-интерфейс Kaspersky CyberTrace в браузере.

   b. Запустите службу Kaspersky CyberTrace.

      Выполните команду `systemctl start cybertrace.service`.

   c. Откройте веб-интерфейс Kaspersky CyberTrace по адресу, указанному в параметре `Configuration > GUISettings > HTTPServer > ConnectionString`, и убедитесь, что страница **Параметры → Потоки данных** содержит только что добавленный поток данных об угрозах и его настройки аналогичны настройкам на хосте DMZ. Также убедитесь, что все остальные потоки данных об угрозах настроены правильно.

   d. На странице **Параметры → Потоки данных** задайте значение **Никогда** для параметра **Частота обновления по умолчанию**.

Синхронизация каталогов, содержащих потоки данных об угрозах (сценарий DMZ)

Для синхронизации потоков данных об угрозах на локальном хосте и на хосте DMZ можно использовать утилиту RSync.

> Если хостом DMZ является хост с ОС Windows, утилиту RSync можно запустить с помощью Cygwin. Порядок установки Cygwin описан в разделе Раздельная установка Kaspersky CyberTrace Service и Feed Utility (Windows).

Чтобы настроить синхронизацию на хосте DMZ, выполните следующие действия:

1. На хосте DMZ настройте компоненты OpenSSH следующим образом:

   a. Выполните следующую команду как root:

      ```
      ssh-host-config
      ```

      На все вопросы можно ответить `Yes`. Смысл операции в том, чтобы запустить демон sshd как службу.

   b. Выполните следующую команду:

      ```
      net start sshd
      ```

Демон sshd автоматически запустится.

Чтобы настроить синхронизацию на локальном хосте, выполните следующие действия:

1. Создайте закрытый ключ и соответствующий открытый ключ.

   Для этого выполните на локальном хосте следующую команду:

   ```
   ssh-keygen -t rsa -q -N '' -f /home/<user>/.ssh/dmz_rsa_key
   ```

   Укажите логин пользователя вместо `<user>`. Ключи будут созданы без пароля.

2. Скопируйте открытый ключ с локального хоста на хост DMZ, для этого выполните следующую команду:

   ```
   ssh-copy-id -i /home/<user>/.ssh/dmz_rsa_key <DMZ_user>@<DMZ_host>
   ```

   После запуска этой команды предлагается ввести пароль для `<DMZ_user>@<DMZ_host>`.

3. Проверьте синхронизацию содержимого каталогов, содержащих потоки данных об угрозах, для этого выполните следующую команду на локальном хосте:

   ```
   rsync -a --delete-before --delay-updates -e "ssh -i /home/<user>/.ssh/dmz_rsa_key"
   <DMZ_user>@<DMZ_host>:/<Path_to_feeds>/ /<Path_to_feeds_on_Local>/
   ```

   В этой команде `<Path_to_feeds_on_Local>` — это путь к каталогу, содержащему потоки данных об угрозах на локальном хосте (а именно, `%service_dir%/feeds`), а `<Path_to_feeds>` — это путь к каталогу, в котором хранятся обновленные потоки данных об угрозах на хосте DMZ.

   Чтобы проверка синхронизации была пройдена, содержимое каталога `<Path_to_feeds_on_Local>` на локальном хосте должно совпадать с содержимым каталога `<Path_to_feeds>` на хосте DMZ.

Обновление Kaspersky CyberTrace с предыдущей версии (сценарий DMZ)

Чтобы обновить Kaspersky CyberTrace и Feed Utility до более новых версий, выполните следующие действия:

1. Обновите Kaspersky CyberTrace на локальном хосте, как описано в разделе Автоматическое обновление в ОС Linux.

2. Переместите файл `kl_feed_util` из каталога `%service_dir%/dmz` на локальном хосте в `%dmz_fu%` на хосте DMZ.

Веб-интерфейс Kaspersky CyberTrace

Веб-интерфейс Kaspersky CyberTrace реализован как HTTP-служба. Этот веб-интерфейс называется веб-интерфейсом Kaspersky CyberTrace (Kaspersky CyberTrace Web).

При вводе в браузере URL веб-интерфейса Kaspersky CyberTrace отображается страница входа.

Для аутентификации пользователей веб-интерфейс Kaspersky CyberTrace использует токены. Токен хранится в файлах cookie и обновляется каждые несколько минут.

После входа становятся доступны другие веб-страницы.

В зависимости от роли пользователя доступны страницы, соответствующие одному из двух режимов:

- **Управление системой**

  Веб-страницы, относящиеся к Kaspersky CyberTrace в целом. Доступны только с ролью «Администратор».

  - **Информационная панель**

    Статистическая информация о работе Kaspersky CyberTrace.

  - **Ретроскан**
  - **Задачи**
  - **Параметры**

    Параметры, относящиеся к Kaspersky CyberTrace в целом.

- **Управление данными**

  Веб-страницы, относящиеся к определенному тенанту. Доступны с ролями «Администратор» или «Менеджер тенанта» для данного тенанта. Частично доступны с ролью «Аналитик» для данного тенанта.

  - **Информационная панель**

    Статистическая информация о работе тенанта.

  - **Поиск**
  - **Индикаторы**
  - **Обнаружения**
  - **Графы расследования**
  - **Параметры**

    Параметры, относящиеся к тенанту.

Переключение режимов веб-интерфейса

*Переключение с режима **Управление системой** на режим **Управление данными** выполняется следующим образом:*

1. В левом меню выберите пункт **Система**.
2. В открывшемся меню в разделе **Управление данными** выберите название тенанта, на который требуется переключиться.

*Переключение с режима **Управление данными** на режим **Управление системой** выполняется следующим образом:*

1. В левом меню нажмите на название текущего тенанта.
2. В открывшемся меню выберите пункт **Система**.

Управление с помощью клавиатуры

Для выполнения действий, для которых обычно требуется мышь, можно использовать клавиатуру.

Можно использовать следующие клавиши:

- **ENTER**

  Нажатие на клавишу **ENTER** подтверждает действие (например, переход на следующую страницу или применение изменений). Эта клавиша эквивалентна нажатию кнопок **Далее** и **Сохранить** в веб-интерфейсе Kaspersky CyberTrace.

- **ESC**

  Нажатие на клавишу **ESC** отменяет действие (например, таким образом можно отменить изменения). Эта клавиша эквивалентна нажатию кнопки **Отмена** в веб-интерфейсе Kaspersky CyberTrace.

Темная тема

При использовании веб-интерфейса Kaspersky CyberTrace вы можете переключиться на темную тему, чтобы снизить нагрузку на глаза.

Чтобы включить темную тему, нажмите на значок **Включить темную тему** (☾) в левой верхней части веб-интерфейса. При включенной темной теме значок превращается в **Включить светлую тему** (☀).

Интеграция с Kaspersky Unified Monitoring and Analysis Platform

Kaspersky CyberTrace для Linux поддерживает интеграцию с Kaspersky Unified Monitoring and Analysis Platform (здесь и далее — «KUMA»). В этой схеме интеграции веб-интерфейс Kaspersky CyberTrace служит встроенным интерфейсом для KUMA, что способствует дальнейшему развитию платформы, предоставляя ключевые функции веб-интерфейса Kaspersky CyberTrace.

Kaspersky CyberTrace отправляет в KUMA следующие страницы веб-интерфейса пользователя в зависимости от роли пользователя KUMA (Администратор или Аналитик). Все приведенные ниже страницы, кроме страницы **Параметры**, доступны для пользователей как с ролью «Администратор», так и с ролью «Аналитик». Страница **Параметры** доступна только с ролью «Администратор»:

- **Информационная панель**

  Отображение этой страницы поддерживается с некоторыми ограничениями. В частности, невозможно просматривать статистику работы Kaspersky CyberTrace в полноэкранном режиме.

- **Поиск**
- **Обнаружения**
- **Индикаторы**
- **Ретроскан**
- **Параметры**

О ролях пользователей

Ролью называется набор прав, определяющий функции Kaspersky CyberTrace, к которым пользователю предоставлен доступ. Каждой локальной учетной записи пользователя при ее создании назначается роль. Роль собственной учетной записи изменить невозможно.

В Kaspersky CyberTrace предусмотрены следующие роли:

- Администратор

  Администраторы могут управлять учетными записями пользователей и настраивать Kaspersky CyberTrace. У администраторов есть доступ ко всем тенантам; они могут настраивать тенанты и просматривать их статистику, индикаторы и обнаружения киберугроз. Администраторы также могут скачивать статистические отчеты. Администраторы могут предоставлять менеджерам тенанта и аналитикам доступ к определенным тенантам или ко всем тенантам, включая тенанты, которые будут добавлены позже. По умолчанию назначается роль Administrator.

- Менеджер тенанта

  У менеджеров тенантов есть доступ ко всем тенантам или к определенным тенантам; менеджеры тенантов могут настраивать тенанты и просматривать их статистику, индикаторы и обнаружения киберугроз. Менеджеры тенантов также могут скачивать статистические отчеты.

  Вы можете назначать роль «Менеджер тенанта», только если на вашем уровне лицензирования доступен режим мультитенантности.

- Аналитик

  У аналитиков есть доступ ко всем тенантам или к определенным тенантам; аналитики могут просматривать статистику тенантов, индикаторы и обнаружения киберугроз. Аналитики также могут скачивать статистические отчеты. Аналитики не могут настраивать тенанты.

Режим **Управление системой** доступен только администраторам; они могут выполнять в этом режиме любые действия. В режиме **Управление данными** состав доступных действий зависит от роли.

Права доступа в режиме управления данными

В режиме **Управление данными** могут работать пользователи с любой ролью. В таблице ниже описаны действия, доступные в этом режиме в зависимости от роли пользователя.

Права доступа в режиме управления данными

Действие	Администратор	Менеджер тенантов	Аналитик
Страница **Информационная панель**			
Просмотр статистики на информационной панели	✓	✓	✓
Настройка информационной панели	✓	✓	✓
Страница **Поиск**			
Поиск конкретного индикатора	✓	✓	✓
Поиск индикаторов в файлах журнала	✓	✓	✓
Поиск хешей файлов	✓	✓	✓
Страница **Индикаторы** → Таблица индикаторов			
Просмотр индикаторов	✓	✓	✓
Поиск индикаторов в таблице индикаторов	✓	✓	✓
Работа со списком ложных срабатываний	✓	✓	✓
Работа со списком **Пользовательский список индикаторов**	✓	✓	✓
Экспорт индикаторов в файл CSV	✓	✓	✓
Страница **Индикаторы** → страница индикатора			
Маркировка индикатора как ложного срабатывания	✓	✓	✓
Удаление индикатора из списка ложных срабатываний	✓	✓	✓
Добавление индикатора в граф расследования	✓	✓	✓
Просмотр обнаружений киберугроз, связанных с индикатором	✓	✓	✓
Копирование данных индикатора в буфер обмена	✓	✓	✓
Просмотр индикатора на Kaspersky Threat Intelligence Portal	✓	✓	✓
Обогащение индикатора данными из Kaspersky Threat Intelligence Portal	✓	✓	✓
Получение публикаций об индикаторе из источников APT или Crimeware	✓	✓	✓
Просмотр контекста индикатора в источниках, которые его содержат	✓	✓	✓
Добавление индикатора в список **Пользовательский список индикаторов**	✓	✓	✓
Присвоение тегов индикатору	✓	✓	✓
Добавление и удаление комментариев к индикатору	✓	✓	✓
Страница **Обнаружения**			
Просмотр обнаружений киберугроз	✓	✓	✓

Действие	Администратор	Менеджер тенантов	Аналитик
Просмотр подробной информации об обнаружении киберугрозы	✓	✓	✓
Копирование данных обнаружения киберугрозы в буфер обмена	✓	✓	✓
Поиск обнаружений киберугроз	✓	✓	✓
Экспорт обнаружений киберугроз в файл CSV	✓	✓	✓
Настройка отображения таблицы обнаружений киберугроз	✓	✓	✓
Страница **Графы расследования**			
Создание, изменение и удаление графов расследования	✓	✓	✓
Добавление токена доступа для обогащения индикаторов из графа расследования	✓	✓	—
Страница **Параметры → Общие**			
Изменение описания тенанта	✓	—	—
Сброс статистики тенанта	✓	—	—
Настройка лимита EPS для тенанта	✓	—	—
Настройка входящих событий	✓	✓	—
Настройка исходящих оповещений об обнаружении индикаторов компрометации	✓	✓	—
Настройка исходящих служебных оповещений	✓	✓	—
Включение и отключение функции API lookup	✓	✓	—
Страница **Параметры → Служебные оповещения**			
Настройка формата служебных оповещений	✓	✓	—
Страница **Параметры → Потоки данных**			
Включение и отключение потоков данных об угрозах	✓	✓	—
Добавление полей контекста в поток данных	✓	✓	—
Страница **Параметры → Отчеты**			
Создание, изменение и удаление задач формирования отчетов для тенанта	✓	✓	—
Включение и отключение задач формирования отчетов	✓	✓	—
Запуск задач формирования отчетов	✓	✓	—
Скачивание сформированных отчетов	✓	✓	—
Проверка подключения к почтовому серверу	✓	✓	—
Страница **Параметры → Источники событий**			
Создание, изменение и удаление источников событий для тенанта	✓	✓	—
Работа с правилами нормализации источников событий	✓	✓	—
Работа с регулярными выражениями источников событий	✓	✓	—
Страница **Параметры → Оповещения об обнаружении индикаторов компрометации**			
Настройка формата оповещений об обнаружении индикаторов компрометации	✓	✓	—
Настройка правил фильтрации для оповещений об обнаружении индикаторов компрометации	✓	✓	—
Настройка контекста оповещений об обнаружении индикаторов компрометации	✓	✓	—

Краткое руководство по использованию Kaspersky CyberTrace

В этом разделе объясняется, как начать работу с Kaspersky CyberTrace сразу после установки. Особое внимание уделяется распространенным сценариям использования Kaspersky CyberTrace и основным функциям программы.

Вход в веб-интерфейс Kaspersky CyberTrace

Чтобы войти в веб-интерфейс Kaspersky CyberTrace, выполните следующие действия:

1. Введите адрес веб-интерфейса Kaspersky CyberTrace в адресной строке браузера.

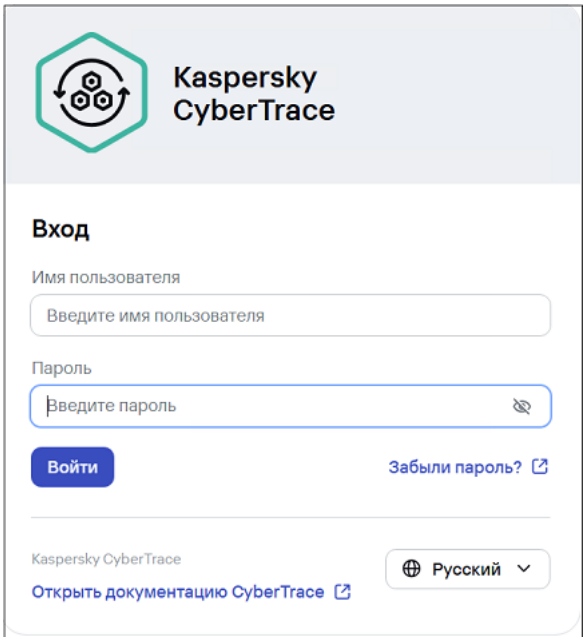
   Откроется окно **входа**.

2. В поле **Имя пользователя** введите свое имя пользователя.

3. В поле **Пароль** введите свой пароль.

4. Нажмите **Войти**.

Дополнительную информацию см. в статье "Вход в веб-интерфейс Kaspersky CyberTrace".



Вход в Kaspersky CyberTrace

Настройка Kaspersky CyberTrace

Чтобы настроить Kaspersky CyberTrace, выполните следующие действия:

1. Перейдите в режим Управление системой.

   Информацию о переключении между режимами веб-интерфейса см. в статье "О веб-интерфейсе Kaspersky CyberTrace".

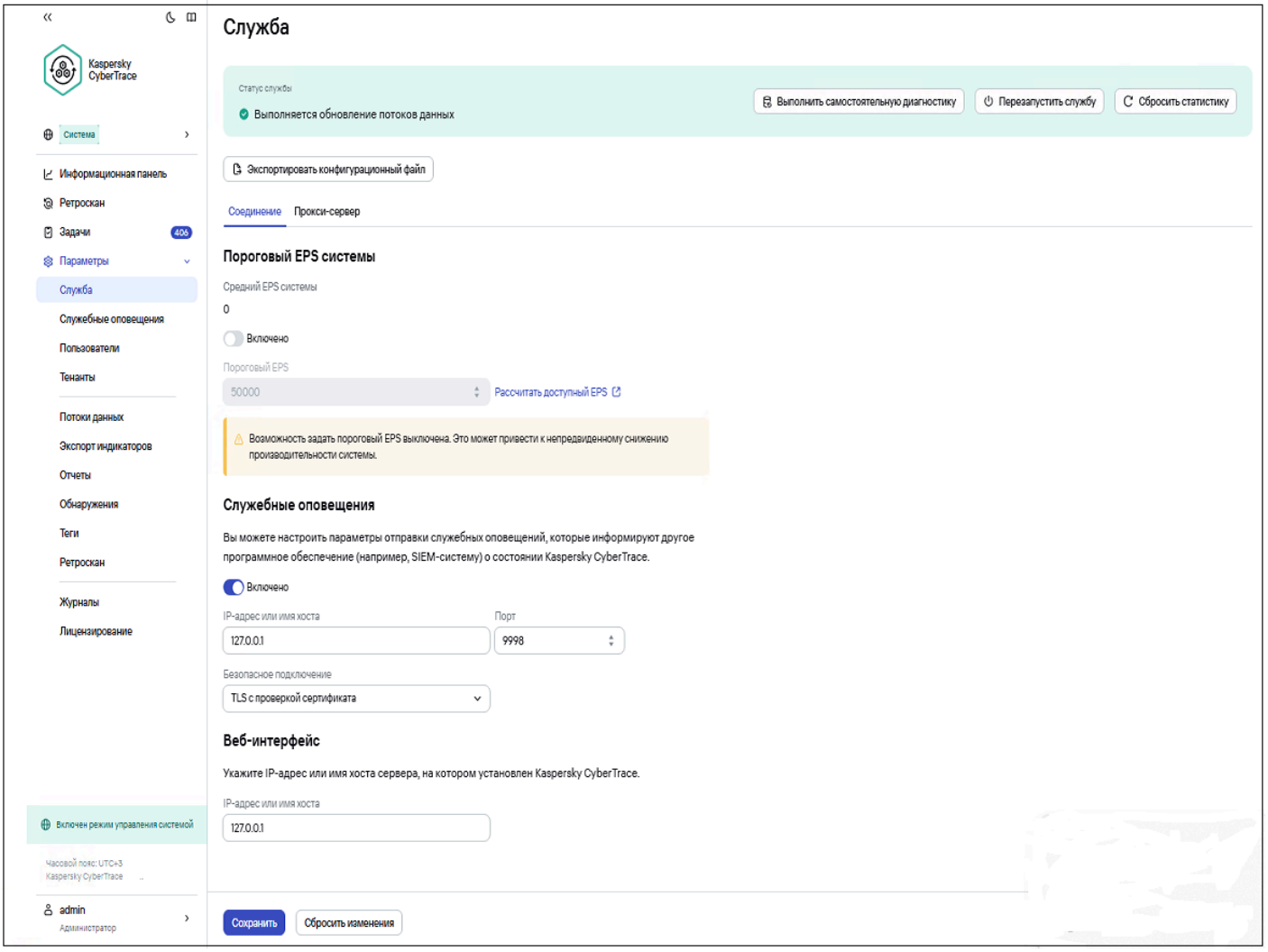
2. Перейдите в раздел **Настройки** → **Служба**.

3. В окне **Служба**:

   - Примените параметры подключения.
   - Примените настройки прокси-сервера.

В окне **Служба** также можно запустить самостоятельную диагностику, перезапустить службу, сбросить статистику и экспортировать конфигурационные файлы.

Дополнительная информация об общих параметрах службы Kaspersky CyberTrace приведена в статье Настройки службы.



Использование распространенных сценариев Kaspersky CyberTrace

В этом разделе приведено краткое описание распространенных сценариев и функций, доступных в Kaspersky CyberTrace.

При работе в веб-интерфейсе Kaspersky CyberTrace потребуется переключаться между двумя режимами, Управление системой и Управление данными, в зависимости от вашей роли и используемого сценария.

Информацию о переключении между двумя режимами см. в статье "О веб-интерфейсе Kaspersky CyberTrace".

Распространенные сценарии работы с потоками данных

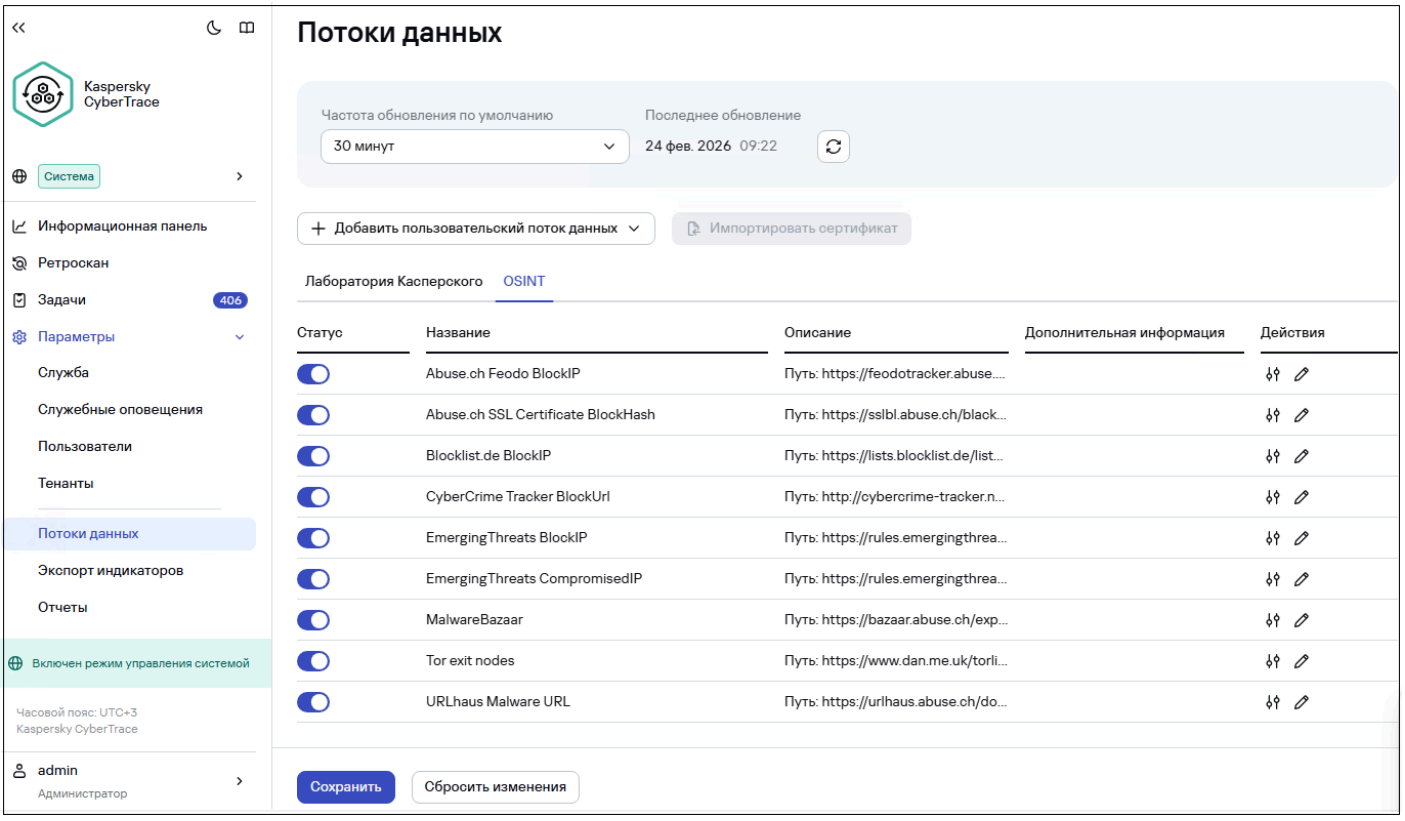
В этой статье описаны распространенные сценарии работы с детекторами.

Использование OSINT feed

Чтобы использовать доступный по умолчанию OSINT feed, выполните следующие действия:

Переключитесь в режим Управление системой и перейдите в раздел **Настройки** → **Потоки данных** → **OSINT**.

Дополнительные сведения о потоках данных OSINT feed приведены в статье О потоках данных об угрозах «OSINT feeds».



Использование OSINT feed

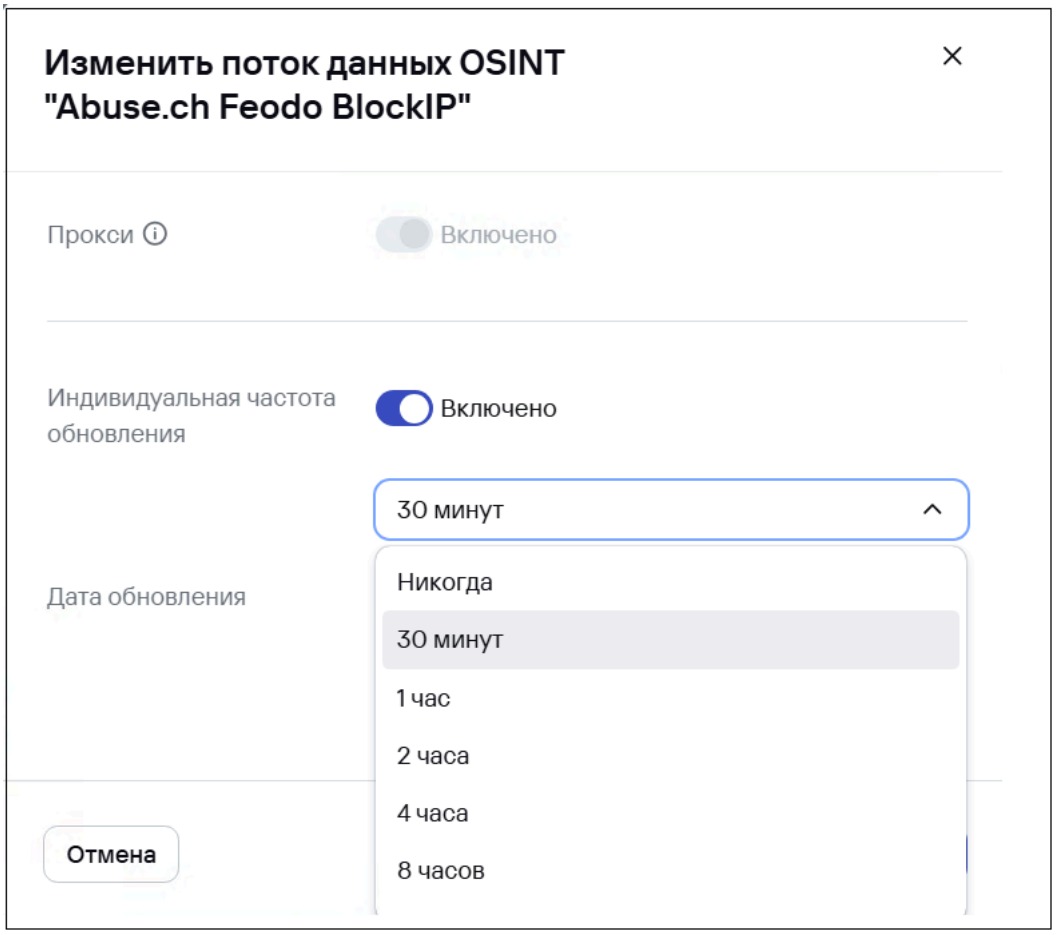
Настройка пользовательской частоты обновления и выбор прокси-сервера

Чтобы настроить пользовательскую частоту обновления и использовать прокси для обновления потоков данных, выполните следующие действия:

1. Перейдите в режим Управление системой и перейдите в раздел **Настройки** → **Потоки данных**.
2. Добавьте пользовательский поток данных или выберите поток данных в таблице потоков данных.
3. В открывшемся окне добавления и редактирования потоков данных включите переключатель **Индивидуальная частота обновления** и введите значение.
4. Если требуется, включите переключатель **Прокси-сервер**.

Более подробные сведения о настройке индивидуальной частоты обновления приведены в статье Запуск обновления потоков данных об угрозах вручную.

Более подробные сведения об использовании прокси-сервера при обновлении потоков данных приведены в статье Использование прокси-сервера для обновления потоков данных.



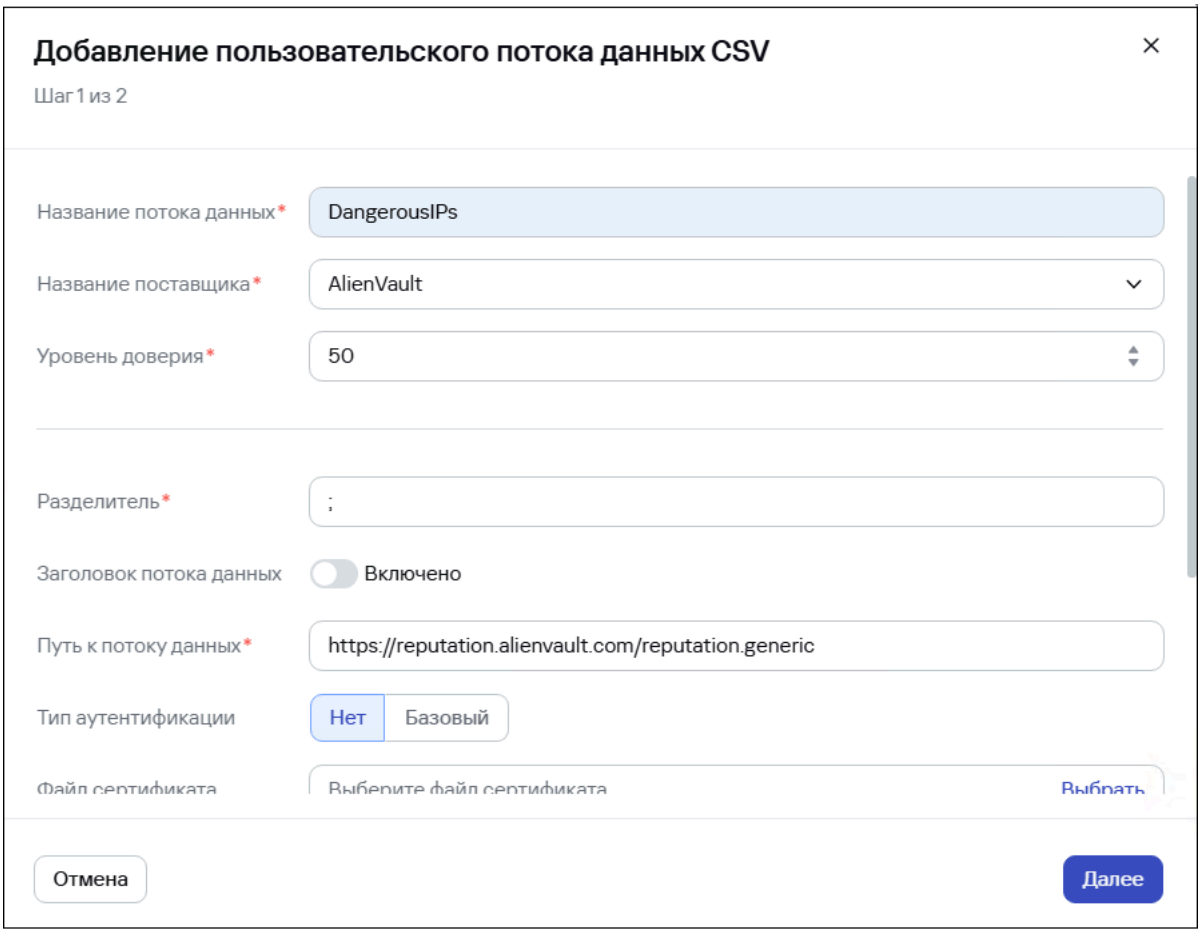
Настройка пользовательской частоты обновления и использование прокси для обновления потоков данных

Добавление пользовательских потоков данных

Чтобы добавить пользовательские или сторонние потоки данных и задать их параметры, выполните следующие действия:

1. Перейдите в режим Управление системой и перейдите в раздел **Настройки** → **Потоки данных**.
2. Нажмите **Добавить пользовательский поток данных**.
3. Выберите тип потока данных.
4. В открывшемся окне добавления пользовательского потока данных задайте параметры добавляемого пользовательского потока данных.
5. Нажмите на кнопку **Add**.

Дополнительную информацию см. в статье Добавление пользовательского или стороннего потока данных.



Добавление пользовательского потока данных об угрозах

Добавление источников событий и проверка входящих событий

Вы можете добавлять и изменять источники событий, проверять входящие события, задавать параметры источников событий, а также указывать правила нормализации и регулярные выражения.

Чтобы добавить источник событий и задать его параметры, выполните следующие действия:

1. Переключитесь в режим Управление данными и перейдите в раздел **Настройки** → **Источники событий**.
2. Нажмите **Добавить источник событий**.

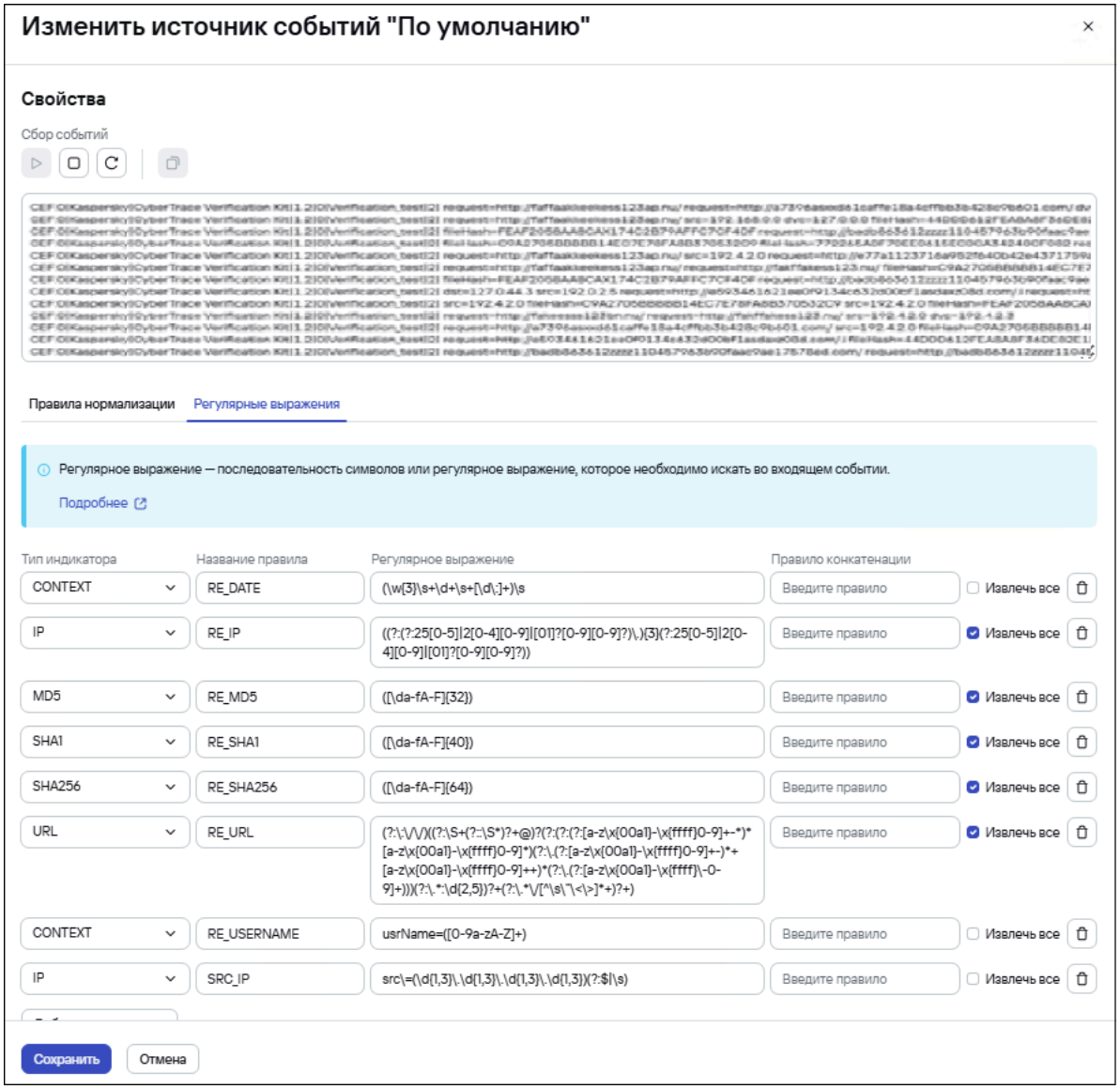
   Запустится мастер **Добавить источник событий**.
3. Задайте параметры нового источника событий.
4. Укажите правила нормализации и регулярные выражения.
5. Нажмите на кнопку **Add**.

Чтобы изменить источник событий и проверить входящие события, выполните следующие действия:

1. Перейдите в раздел **Настройки** → **Источники событий**.
2. Нажмите на кнопку (Edit) рядом с интересующим вас источником событий.

   Откроется окно редактирования источника событий.
3. Измените правила нормализации и регулярные выражения.
4. В разделе **Свойства** проверьте входящие события, нажав **Начать анализ событий**.

Дополнительную информацию см. в статье "Настройка источников событий тенанта".



Изменение источника событий

Просмотр статистики Kaspersky CyberTrace на информационной панели

На информационной панели отображается статистика работы Kaspersky CyberTrace. Кроме того, она содержит ряд виджетов.

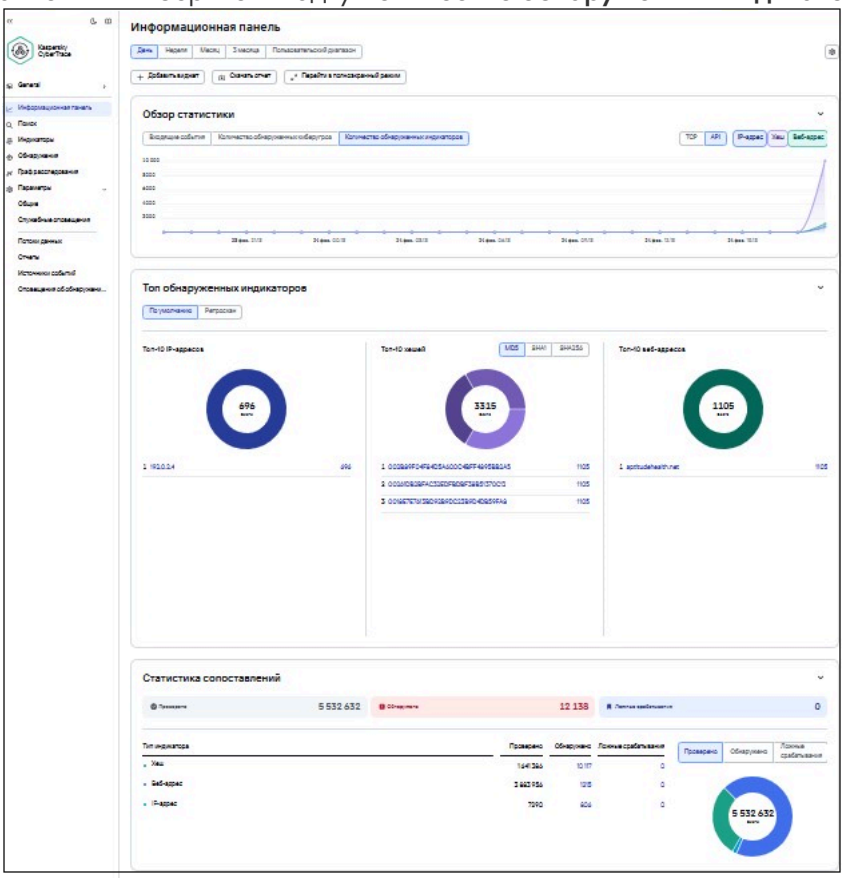
Просмотр статистики обнаружения киберугроз с помощью IoC

Чтобы просмотреть статистику обнаружения киберугроз с помощью IoC, выполните следующие действия:

1. Переключитесь в режим Управление данными и перейдите в раздел **Информационная панель**.

   Откроется окно **Dashboard**.

2. В разделе **Обзор статистики** выберите вкладку **Количество обнаруженных индикаторов**.



Просмотр статистики на информационной панели

Просмотр пересечения потоков данных

Чтобы просмотреть пересечения потоков данных, выполните следующие действия:

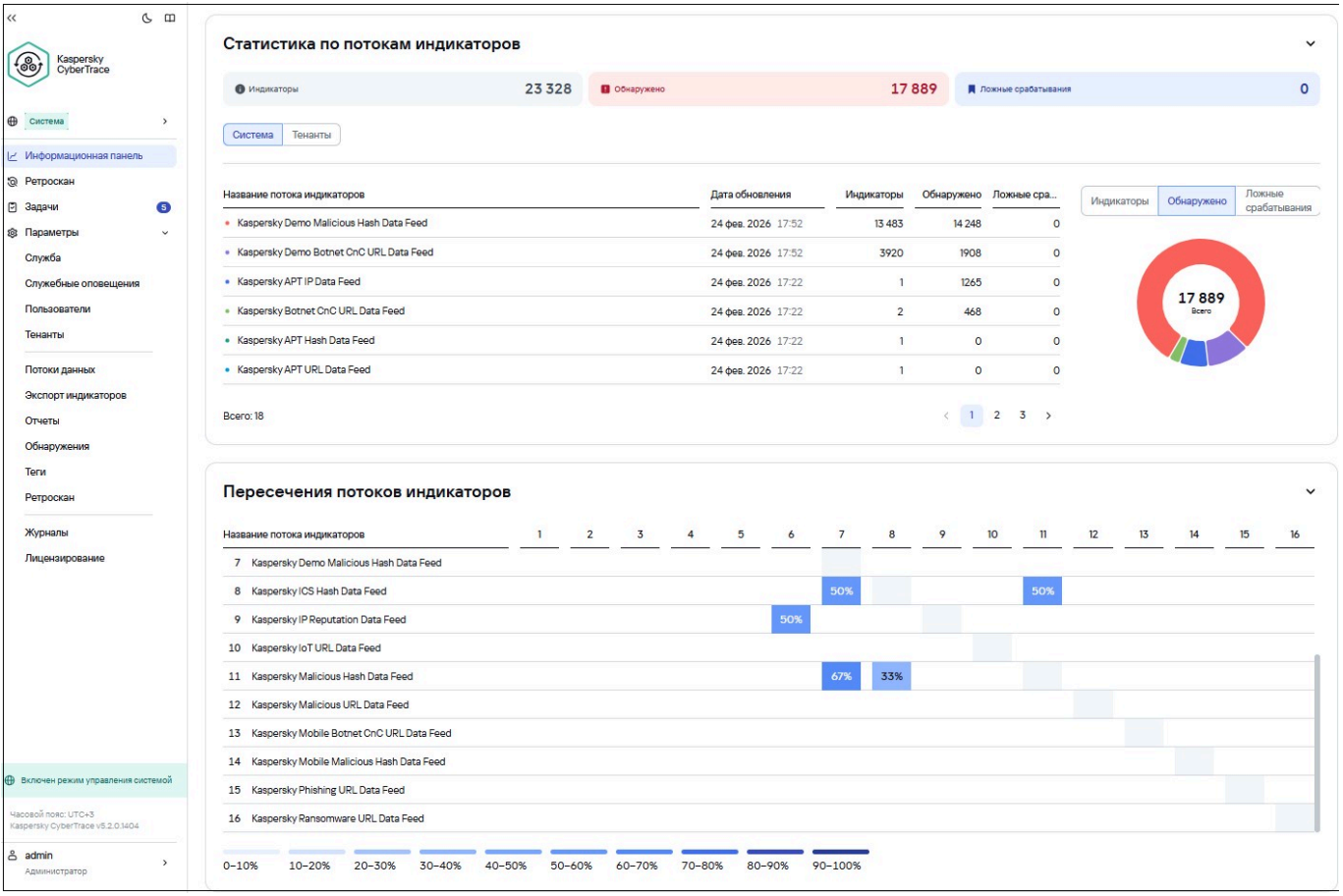
1. Переключитесь в режим Управление данными и перейдите в раздел **Информационная панель**.

   Откроется окно **Dashboard**.

2. Перейдите в раздел **Пересечения источников данных об угрозах**.

   На информационной панели отображается

виджет, который показывает процент пересечения источников данных об угрозах.



Пересечения потоков индикаторов

Распространенные сценарии работы с индикаторами

В этой статье описаны распространенные сценарии работы с индикаторами.

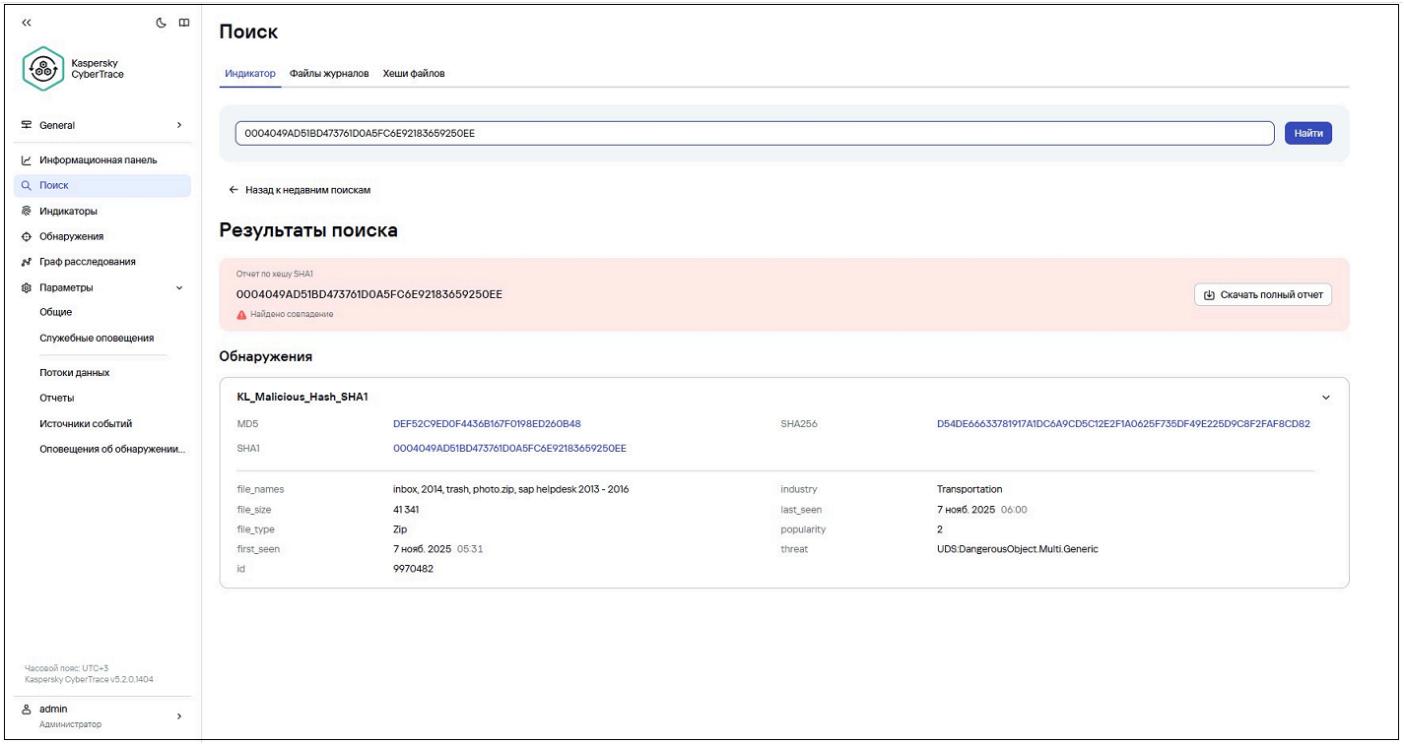
Поиск конкретного индикатора

Чтобы найти информацию о конкретном индикаторе, выполните следующие действия:

1. Переключитесь в режим Управление данными и перейдите в раздел **Поиск**.
   Откроется окно **Search**.
2. Выберите вкладку **Indicator**.
3. В поле **Поиск** введите хеш, IP-адрес или URL-адрес.
4. Нажмите на кнопку **Search**.

Появится результат поиска.

Дополнительную информацию см. в статье "Поиск индикаторов".



Поиск индикаторов

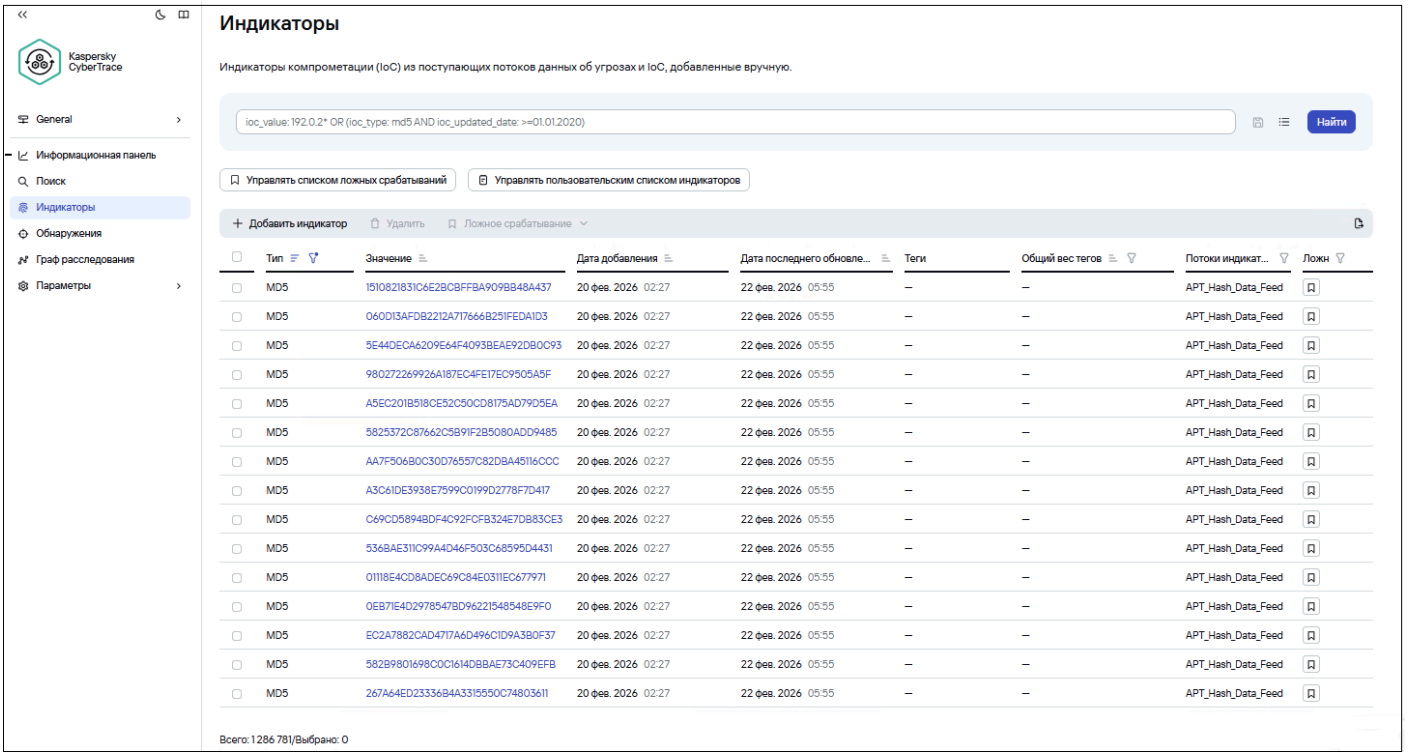
Наблюдение за полной базой данных IoC

Чтобы просмотреть полный список индикаторов, имеющихся в базе данных, выполните следующие действия:

Переключитесь в режим Управление данными и перейдите в раздел **Индикаторы**.

В окне **Индикаторы** отобразится таблица индикаторов.

Дополнительную информацию см. в статье "Просмотр индикаторов".



Просмотр индикаторов

Поиск IoC с использованием синтаксиса поиска

Для поиска индикаторов в базе данных выполните следующие действия:

1. Переключитесь в режим Управление данными и перейдите в раздел **Индикаторы**.

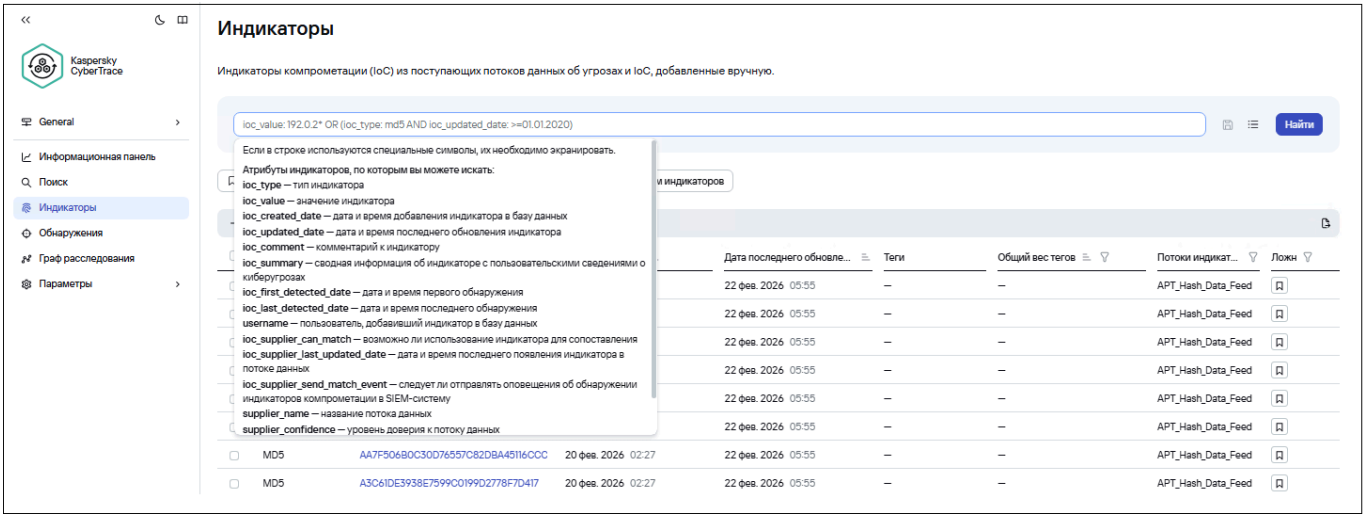
   Откроется окно **Indicators**.

2. В поле **Поиск** введите запрос с использованием синтаксиса поиска.

3. Нажмите на кнопку **Поиск**, чтобы начать поиск.

   В окне **Индикаторы** отобразится список индикаторов, совпавших с указанной строкой.

   Дополнительную информацию см. в статье "Поиск индикаторов в таблице индикаторов".



Поиск IoC с использованием синтаксиса поиска

Просмотр сведений об индикаторах и добавление тегов и комментариев

Чтобы просмотреть подробную информацию об индикаторах и добавить теги и комментарии, выполните следующие действия:

1. Переключитесь в режим Управление данными и перейдите в раздел **Индикаторы**.

   Откроется окно **Indicators**.

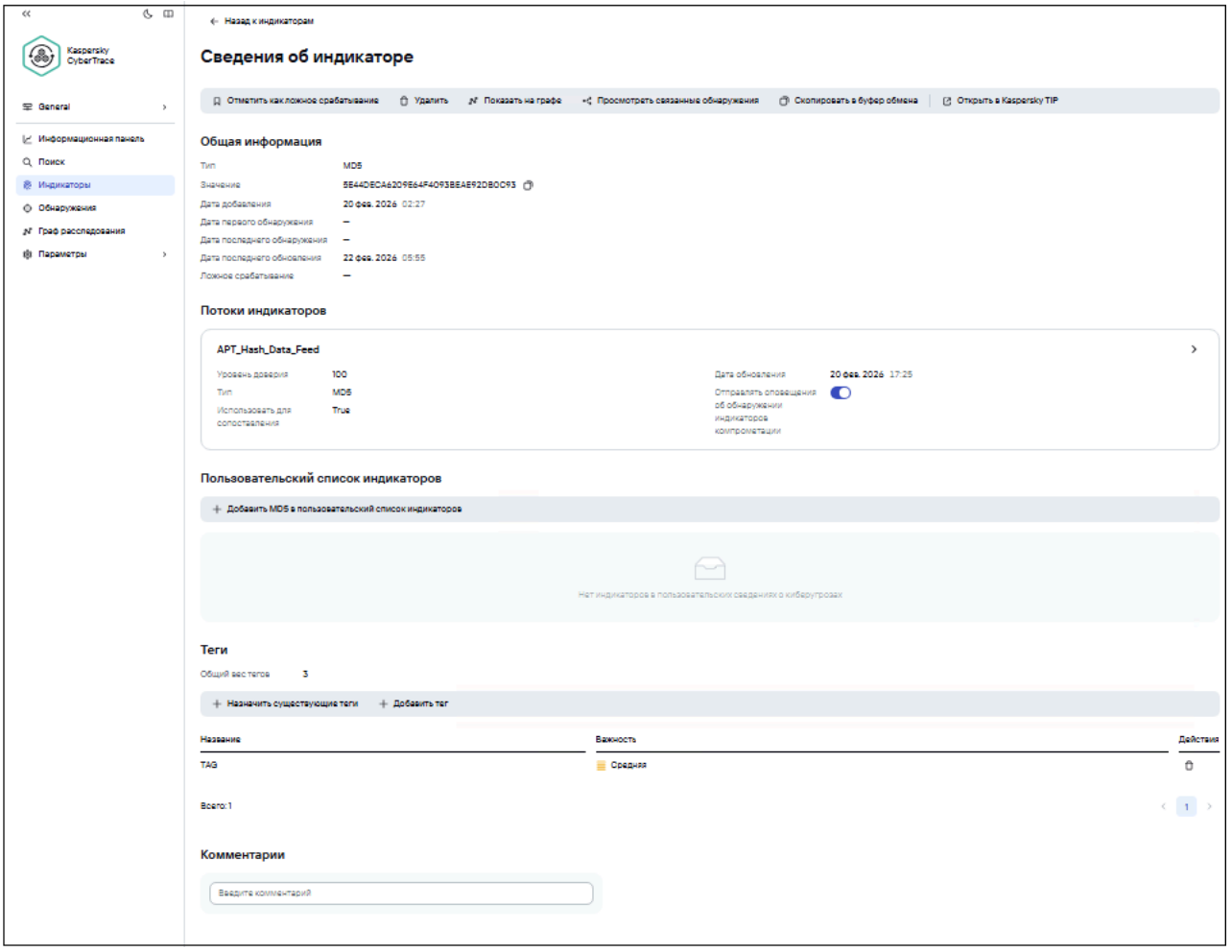
2. Выберите нужный индикатор в таблице индикаторов.

   Откроется окно **Подробности об индикаторе**, в котором отображается подробная информация о выбранном индикаторе.

3. В разделе **Теги** добавьте теги.

4. Если требуется, добавьте комментарии в разделе **Комментарии**.

Дополнительную информацию см. в статье "Просмотр подробной информации об индикаторах".



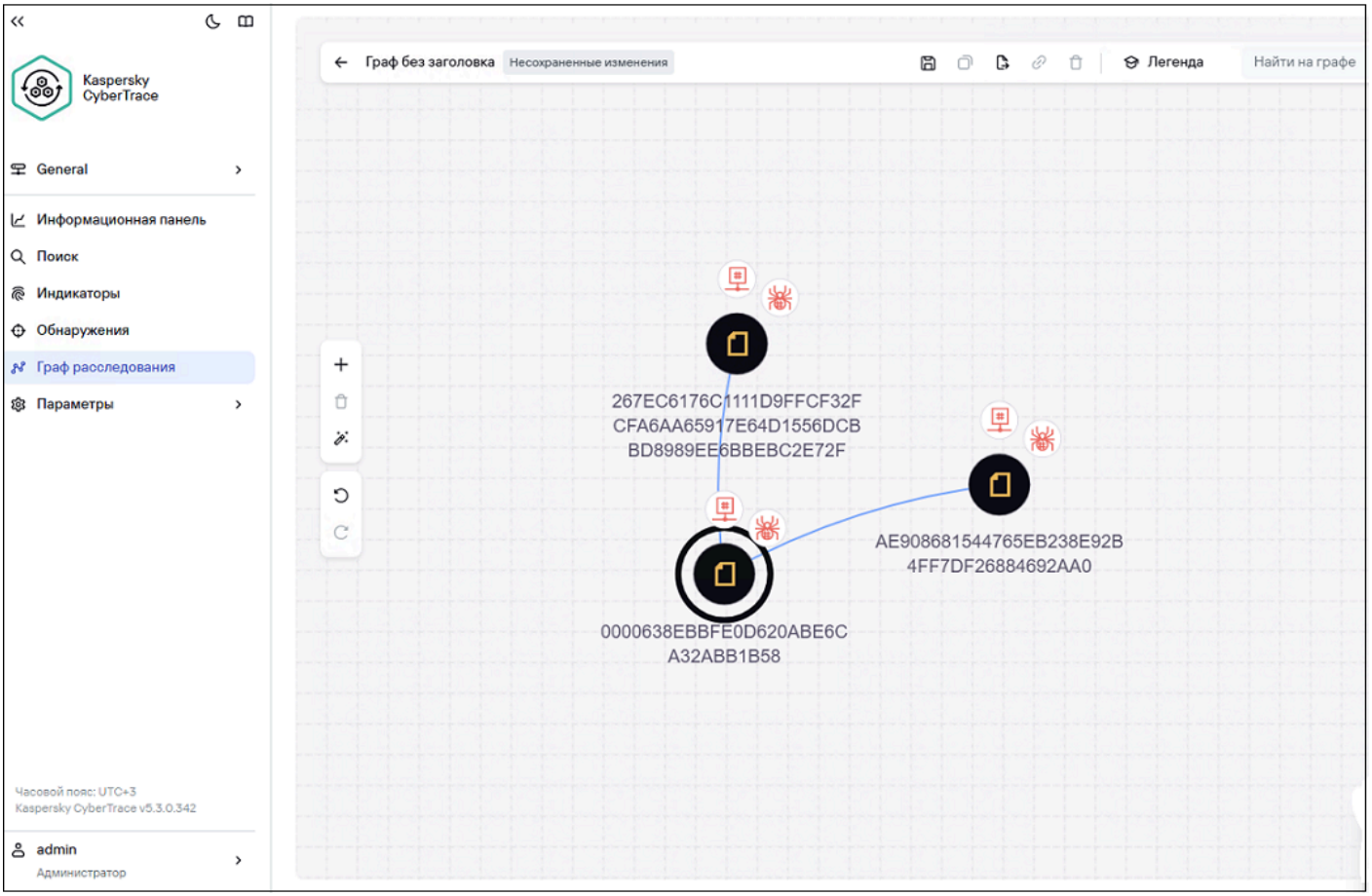
Просмотр подробностей об индикаторах

Изучение связей IoC на графе расследования

Чтобы визуализировать информацию об индикаторах и их связях на графе расследования,

переключитесь в режим Управление данными и перейдите в раздел **Граф расследования.**

Дополнительную информацию см. в статье "Использование графов".



Просмотр графа расследования

Просмотр результатов ретроспективного сканирования для новых IoC

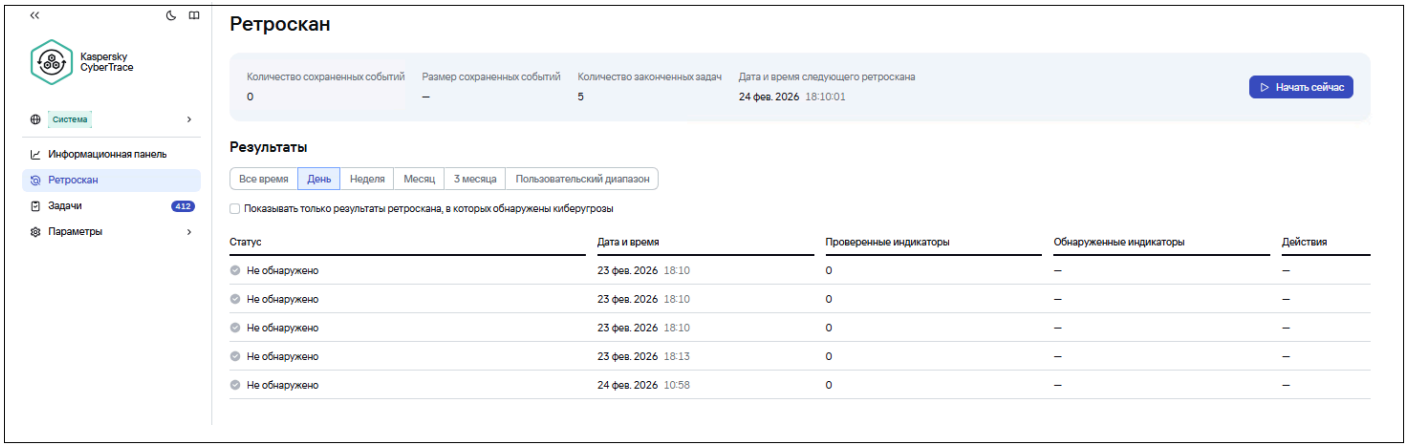
Для просмотра результатов ретроспективного сканирования, выполните следующие действия:

1. Переключитесь в режим Управление системой и перейдите в раздел **Ретроскан**.

   Откроется окно **Ретроскан**.

2. Нажмите на кнопку **Начать сейчас**, чтобы запустить ретроспективное сканирование.

Дополнительную информацию см. в статье "Просмотр результатов ретроспективного сканирования".



Просмотр результатов ретроспективного сканирования

Экспорт индикаторов для использования их в качестве динамического списка блокировки для NGFW

Чтобы экспортировать индикаторы для интеграции в ваш NGFW, выполните следующие действия:

1. Переключитесь в режим Управление системой и перейдите в раздел **Настройки** → **Экспорт индикаторов**.

   Откроется окно **Экспорт индикаторов**.

2. Нажмите **Добавить задачу** и выберите свой NGFW.

   Откроется окно **Add indicators export task**.

3. Укажите свойства задачи.

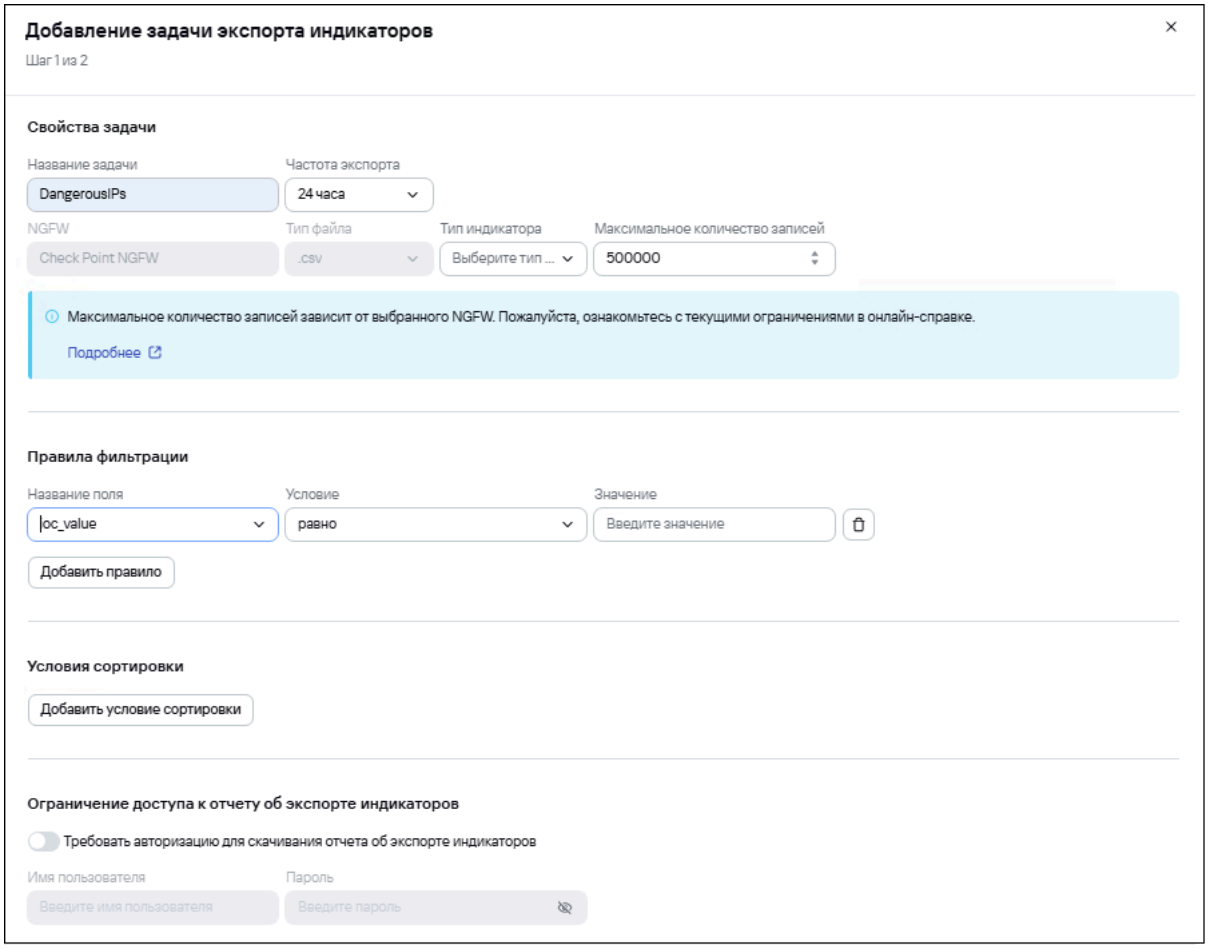
4. Нажмите на кнопку **Next**.

5. В открывшемся окне **Предварительный просмотр экспорта** просмотрите файл экспорта.

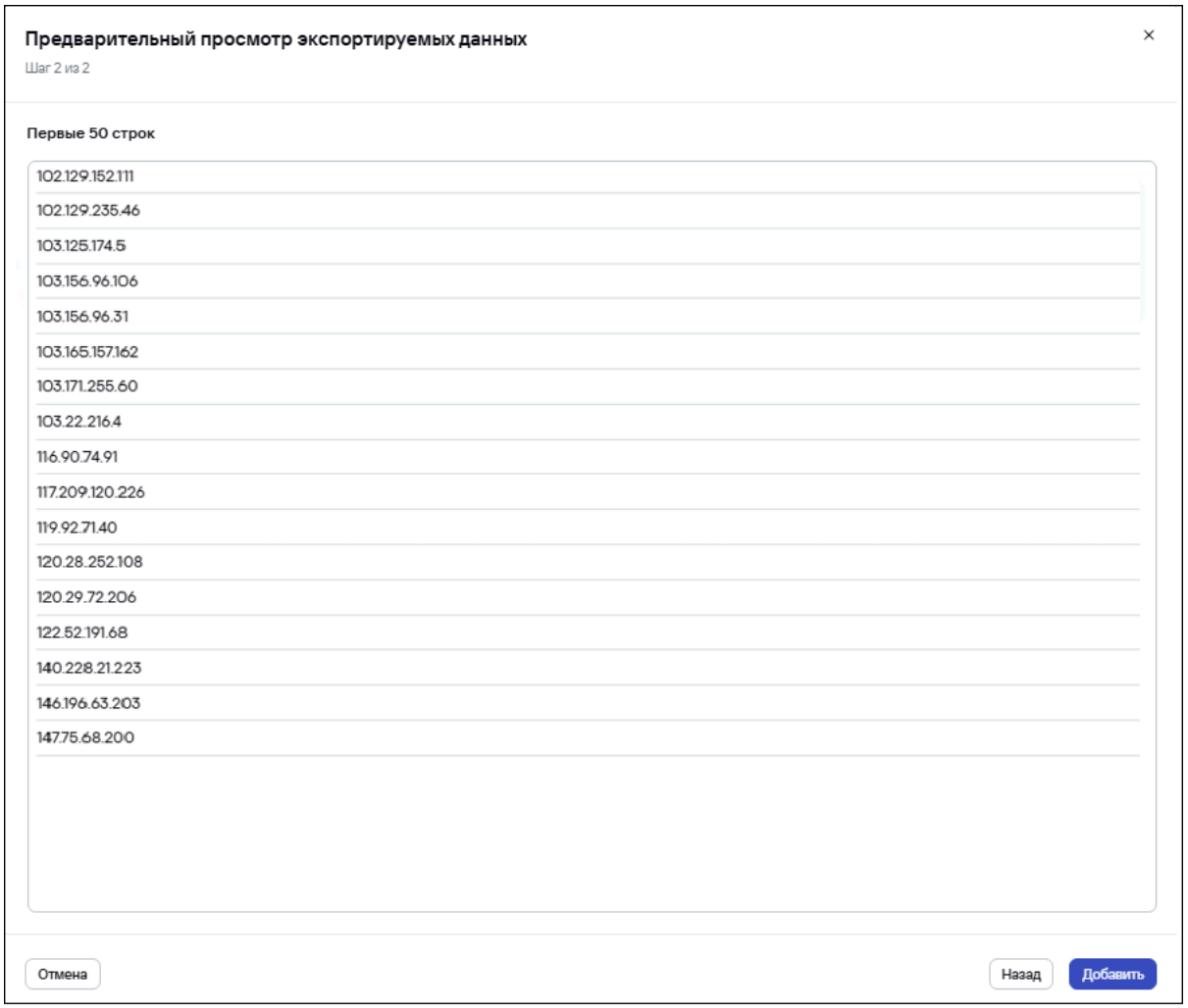
6. Нажмите на кнопку **Add**.

Будет создана задача экспорта, и индикаторы будут экспортированы в созданный файл.

Дополнительную информацию см. в статье "Экспорт индикаторов в NGFW".



Указание свойств задачи экспорта



Предварительный просмотр экспорта

Распространенные сценарии работы с обнаружениями киберугроз

В этой статье описаны распространенные сценарии работы с обнаружениями киберугроз.

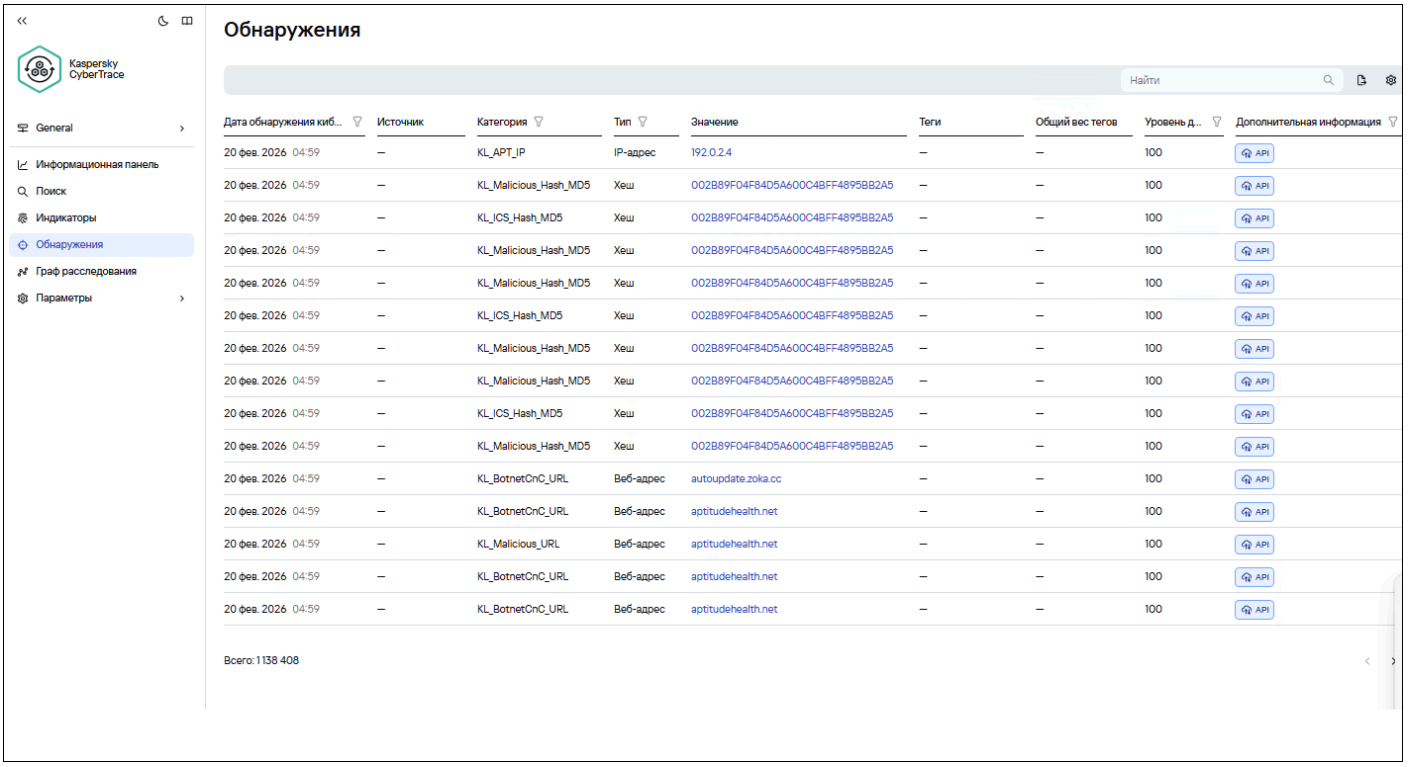
Проверка обнаружений киберугроз IoC во входящих событиях

Чтобы просмотреть входящие события, которые привели к обнаружению киберугрозы, выполните следующие действия:

1. Переключитесь в режим Управление данными и перейдите в раздел **Обнаружение киберугроз**.

2. В открывшемся окне **Обнаружение киберугроз** просмотрите список обнаружений киберугроз.

Дополнительную информацию см. в статье "Просмотр обнаружений киберугроз".



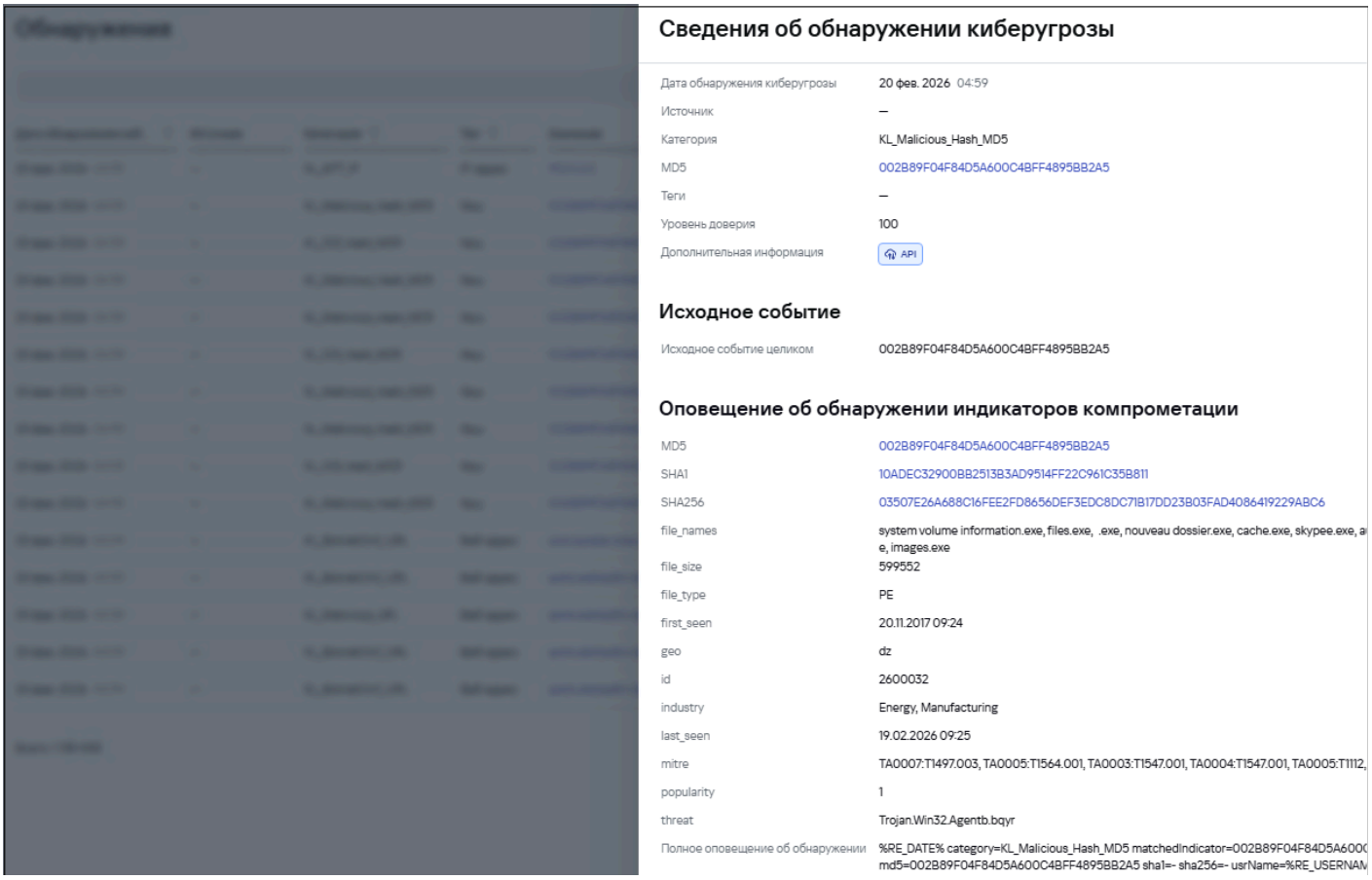
Просмотр обнаруженных киберугроз

Просмотр сведений об отдельном обнаружении киберугрозы

Чтобы просмотреть подробные сведения о отдельном обнаружении киберугрозы, выполните следующие действия:

1. Переключитесь в режим Управление данными и перейдите в раздел **Обнаружение киберугроз**.
2. В открывшемся окне **Обнаружения киберугроз** выберите обнаружение киберугрозы.
3. В открывшемся окне **Сведения об обнаружении киберугрозы** просмотрите информацию об обнаружении киберугрозы.

Дополнительную информацию см. в статье "Просмотр обнаружений киберугроз".



Просмотр сведений об обнаружении киберугрозы

Создание регулярного пользовательского отчета по статистике

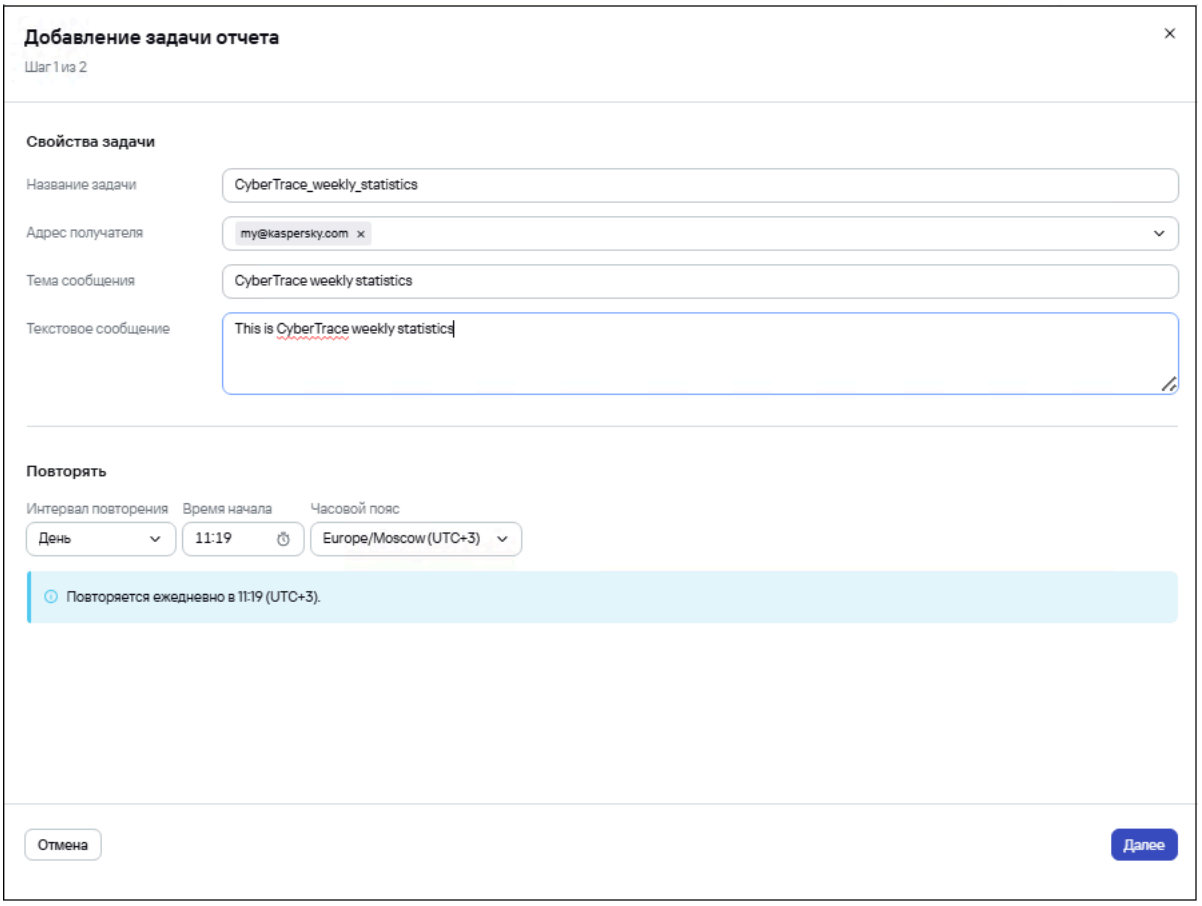
С помощью задач можно отправлять пользовательские отчеты по электронной почте, а также редактировать текст сообщений и составлять расписание отправки.

Чтобы создать задачу отправки статистических отчетов, выполните следующие действия:

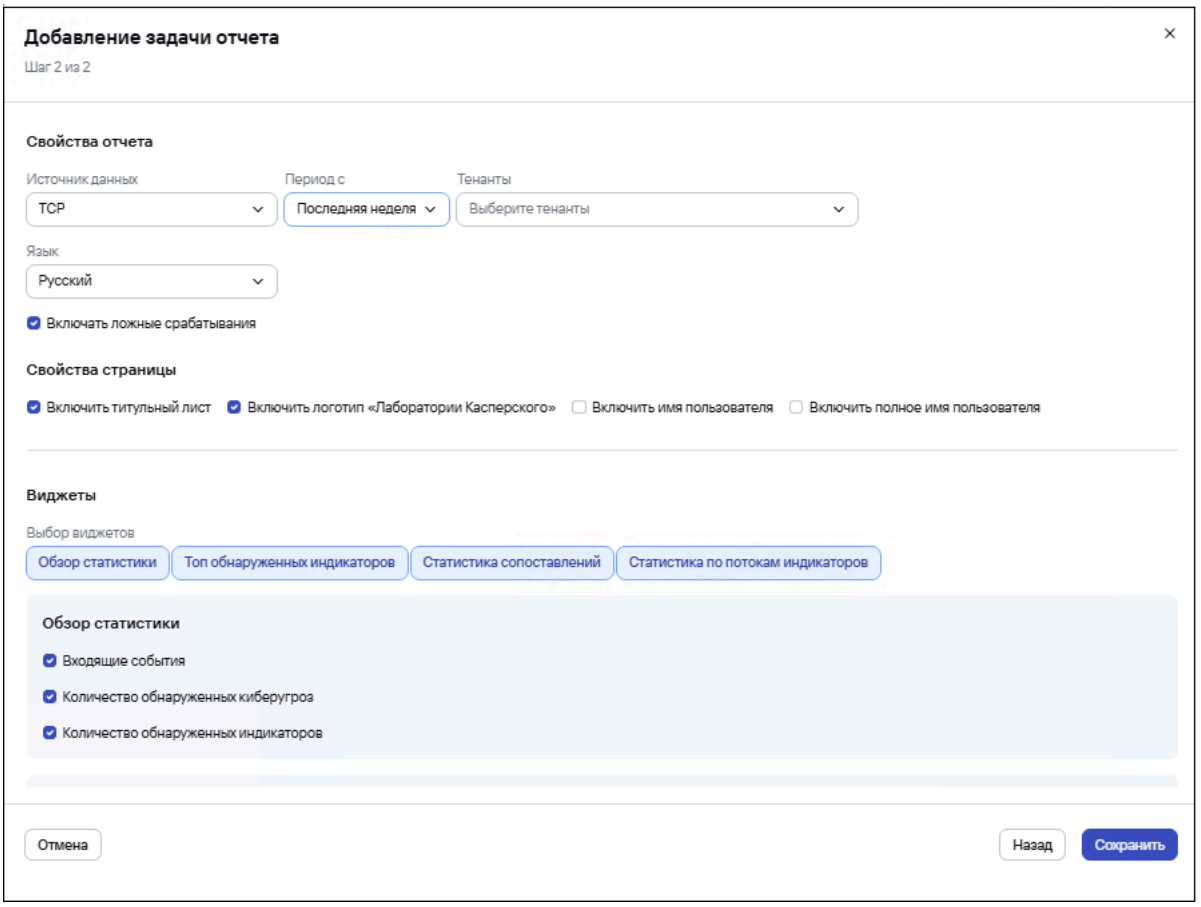
1. Перейдите в режим Управление системой и перейдите в раздел **Настройки** → **Отчеты**.
2. В открывшемся окне **Отчеты** нажмите кнопку **Добавить задачу**.
3. В окне **Добавить задачу отчета** укажите свойства задачи.
4. Нажмите на кнопку **Next**.
5. Настройте свойства отчета.
6. Нажмите на кнопку **Save**.

Задача отчета создана.

Дополнительную информацию см. в статье "Настройка отчетов".

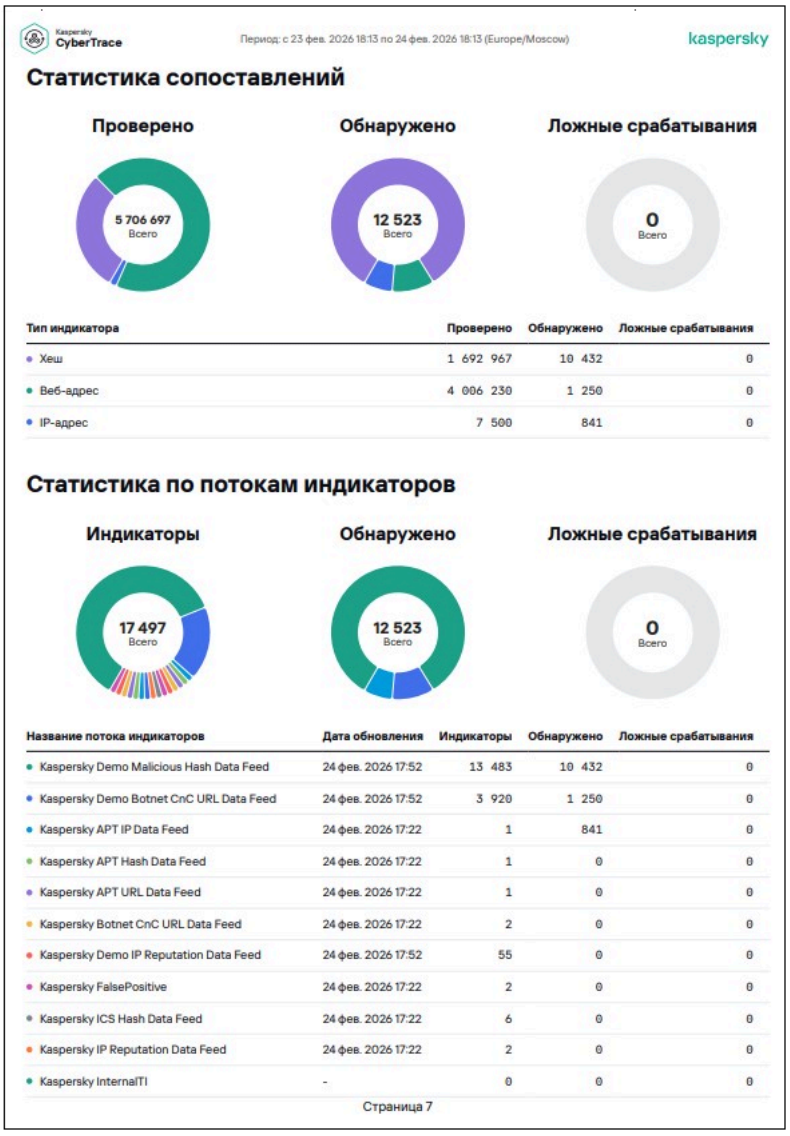


Указание свойств задачи отчета



Настройка параметров отчета

На рисунке ниже показан пример статистического отчета:



Kaspersky CyberTrace

Период: с 23 фев. 2026 18:13 по 24 фев. 2026 18:13 (Europe/Moscow)

kaspersky

Статистика сопоставлений

Проверено

Обнаружено

Ложные срабатывания

Тип индикатора	Проверено	Обнаружено	Ложные срабатывания
Хеш	1 692 967	10 432	0
Веб-адрес	4 006 230	1 250	0
IP-адрес	7 500	841	0

Статистика по потокам индикаторов

Индикаторы

Обнаружено

Ложные срабатывания

Название потока индикаторов	Дата обновления	Индикаторы	Обнаружено	Ложные срабатывания
Kaspersky Demo Malicious Hash Data Feed	24 фев. 2026 17:52	13 483	10 432	0
Kaspersky Demo Botnet CnC URL Data Feed	24 фев. 2026 17:52	3 920	1 250	0
Kaspersky APT IP Data Feed	24 фев. 2026 17:22	1	841	0
Kaspersky APT Hash Data Feed	24 фев. 2026 17:22	1	0	0
Kaspersky APT URL Data Feed	24 фев. 2026 17:22	1	0	0
Kaspersky Botnet CnC URL Data Feed	24 фев. 2026 17:22	2	0	0
Kaspersky Demo IP Reputation Data Feed	24 фев. 2026 17:52	55	0	0
Kaspersky FalsePositive	24 фев. 2026 17:22	2	0	0
Kaspersky ICS Hash Data Feed	24 фев. 2026 17:22	6	0	0
Kaspersky IP Reputation Data Feed	24 фев. 2026 17:22	2	0	0
Kaspersky InternalTI	-	0	0	0

Страница 7

Пример статистического отчета

Руководства пользователя

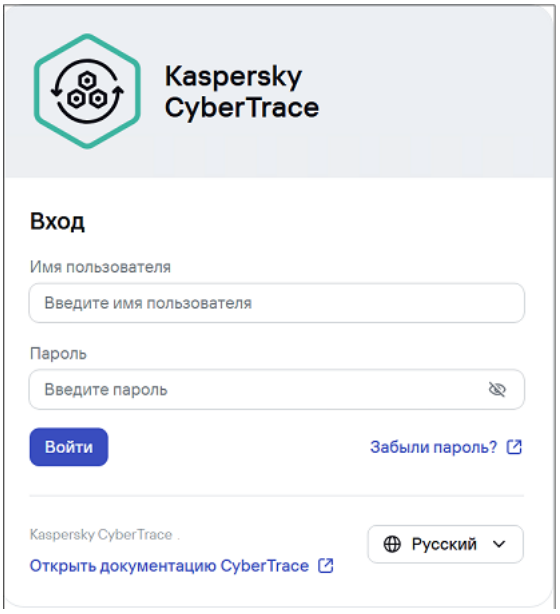
В этой главе представлена информация об использовании веб-интерфейса Kaspersky CyberTrace и приложений для SIEM-систем.

Использование веб-интерфейса Kaspersky CyberTrace

В этом разделе описывается веб-интерфейс пользователя (веб-интерфейс) Kaspersky CyberTrace.

Вход в веб-интерфейс Kaspersky CyberTrace

Веб-интерфейс Kaspersky CyberTrace требует аутентификации. Пользователи, не прошедшие аутентификацию, перенаправляются на страницу входа. Для аутентификации необходимо указать действительное имя локальной или доменной учетной записи и пароль.



Страница **Вход**

Чтобы войти в веб-интерфейс Kaspersky CyberTrace с доменной учетной записью, включите и настройте использование доменных учетных записей пользователей и аутентификацию LDAP.

При неиспользовании веб-интерфейса Kaspersky CyberTrace в течение более пяти минут сессия истекает и вход в систему необходимо повторить.

Если не удалось войти в систему под своим именем пользователя пять раз подряд, необходимо подождать 60 секунд, прежде чем повторить попытку.

Учетные данные

После установки Kaspersky CyberTrace для входа в веб-интерфейс Kaspersky CyberTrace можно использовать предустановленную учетную запись.

Для входа в Kaspersky CyberTrace из учетной записи «Аналитик» запросите учетные данные у администратора.

Сброс пароля учетной записи «Аналитик»

Возможные действия пользователя зависят от его роли.

Смена пароля

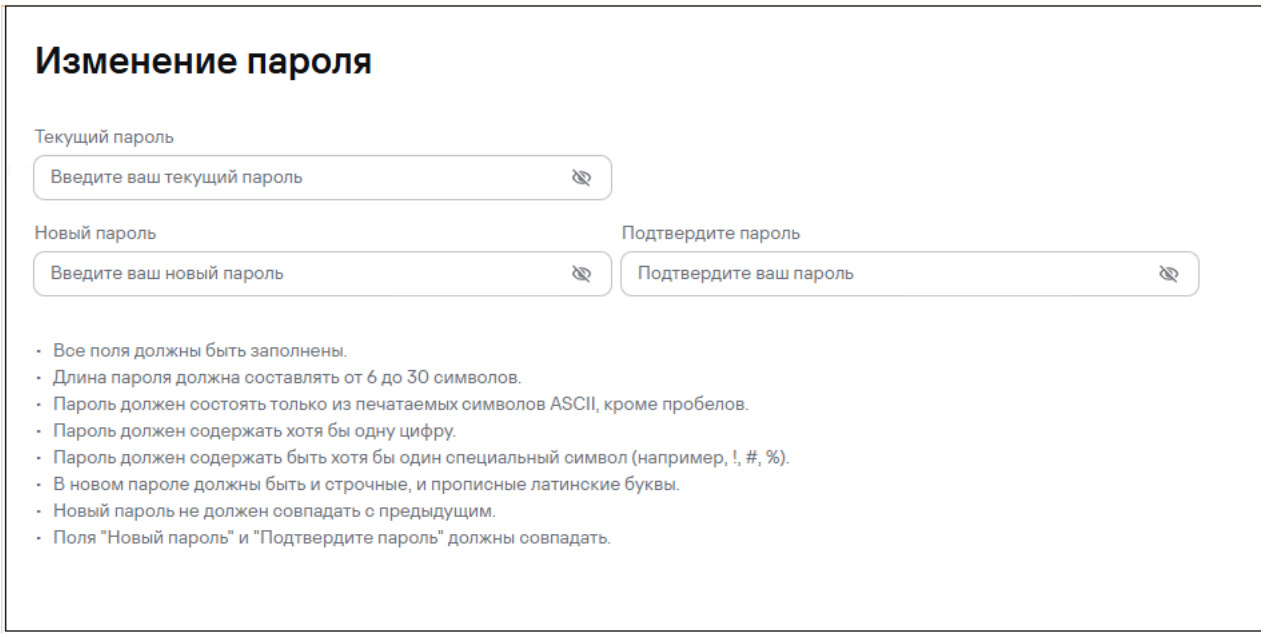
Пользователь, вошедший в систему, может изменить пароль своей учетной записи в любое время.

> При входе в систему в качестве доменного пользователя изменить пароль средствами веб-интерфейса Kaspersky CyberTrace невозможно.

Чтобы изменить пароль учетной записи,

1. В левом нижнем углу страницы нажмите на значок пользователя (👤) и свое имя, затем нажмите **Изменить пароль**.
2. В поле **Текущий пароль** укажите ваш текущий пароль.
3. В полях **Новый пароль** и **Подтвердите пароль** укажите новый пароль.

Пароль должен содержать от 6 до 30 символов ASCII: в нем должна быть хотя бы одна большая латинская буква, одна маленькая латинская буква, одна цифра и один символ другого типа (например, запятая, восклицательный знак или знак №). Новый пароль не должен совпадать с текущим.



Страница **Изменение пароля**

Просмотр статистики на информационной панели

Веб-интерфейс Kaspersky CyberTrace открывается на странице **Информационная панель**. На информационной панели отображается статистика работы Kaspersky CyberTrace.

Обратите внимание, что если служба Kaspersky CyberTrace работает в режиме ReplyBack mode или Log Scanner используется в режиме отчета (с параметром командной строки `-r` или `--report`), Kaspersky CyberTrace не ведет статистику оповещений об обнаружении индикаторов компрометации и на информационной панели не отображается соответствующая статистика. Чтобы сохранять статистику обнаружений киберугроз в режиме «ReplyBack mode», используйте флаг X-KF-SaveStatistic.

При переходе с демонстрационных потоков данных об угрозах на коммерческие потоки данных об угрозах загрузка индикаторов и обновление статистики занимает некоторое время. В течение этого времени на информационной панели может отображаться неполная информация.

Отличия в зависимости от режима пользовательского интерфейса

Информационная панель доступна как в режиме **Управление системой**, так и в режиме **Управление данными**. В зависимости от режима веб-интерфейса Kaspersky CyberTrace виджеты на информационной панели меняются, как описано в следующей таблице.

Отличия виджетов в зависимости от режима веб-интерфейса Kaspersky CyberTrace

	Режим Управление системой	Режим Управление данными
Доступность для пользователей с различными ролями	Виджеты доступны только администраторам.	У администраторов есть доступ к виджетам любого тенанта. У менеджеров тенантов и аналитиков есть доступ к виджетам только тех тенантов, к которым им был предоставлен доступ.
Отображение информации о тенантах	На виджетах отображается агрегированная информация для всех тенантов. Если определенный виджет это позволяет, можно переключить его на отображение информации для выбранных тенантов.	На виджетах отображается информация о тенанте, выбранном в левом меню.
Интерактивность	Виджеты не интерактивны.	Виджеты интерактивны. По нажатию на несколько индикаторов или обнаружений выполняется переход на соответствующую страницу, на которой применен соответствующий фильтр.
Настраиваемые виджеты	Настраиваемые виджеты недоступны.	Можно добавить настраиваемые виджеты.

Загрузка статистических отчетов

Отчет со статистикой обнаружений киберугроз доступен для скачивания в формате PDF. Файл отчета имеет имя вида `report_<дата>.pdf`.

Чтобы скачать отчет, выполните следующие действия:

1. Нажмите на кнопку **Скачать отчет**.
2. Настройте отчет, применив к нему параметры отчетности.
3. Нажмите на кнопку **Скачать**.

Отчет содержит те же данные, которые отображались в веб-интерфейсе на момент инициирования скачивания.

Настройка информационной панели

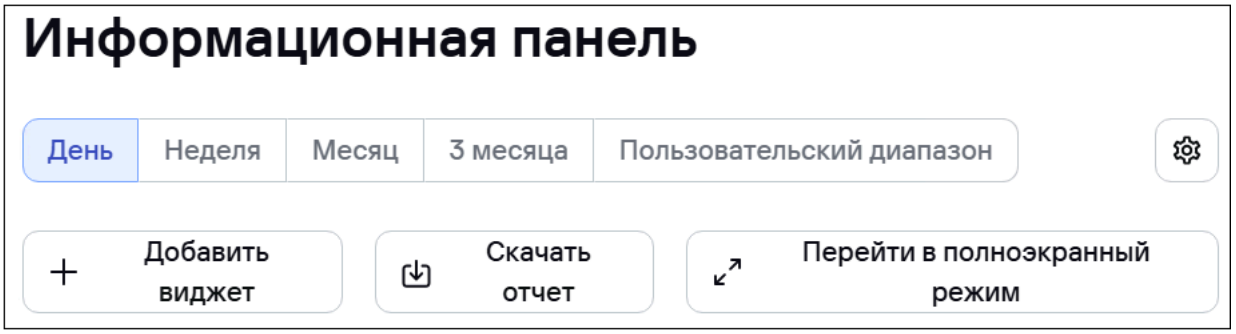
При просмотре страницы **Информационная панель** можно изменять отображение виджетов, как описано в этом разделе.

Указание периода времени для отображения статистики

Период времени для отображения статистики можно указать, выбрав один из следующих вариантов:

- **День** (24 часа)
- **Неделя** (7 дней)
- **Месяц** (31 день)
- **3 месяца** (93 дня)

- **Пользовательский диапазон**



Страница **Информационная панель**. Временные диапазоны для отображения статистики

Включение автоматического обновления данных

Существует возможность включить автоматическое обновление данных на регулярной основе. В этом случае Kaspersky CyberTrace раз в минуту обновляет данные на информационной панели. Если включено автоматическое обновление и роль учетной записи — «Аналитик», сеанс не истечет, пока открыта информационная панель.

Чтобы включить автоматическое обновление данных, выполните следующие действия:

1. Нажмите на значок ⚙ (**Настроить информационную панель**).
2. Включите переключатель **Обновлять панель автоматически**.

По умолчанию этот параметр выключен.

Включение дополнительных виджетов

По умолчанию виджет **Топ обнаруженных индикаторов** отключен, как и возможность добавления пользовательских виджетов.

Чтобы включить эти виджеты:

1. Нажмите на значок ⚙ (**Настроить информационную панель**).
2. Включите переключатель **Включить дополнительные виджеты**.

Отображение статистики

В этом разделе можно выбрать следующие виды статистики для отображения на информационной панели:

- Статистика получения данных по TCP.
- Статистика получения данных через общедоступные API.
- Суммарная статистика получения данных по TCP и через общедоступные API.

Для отображения статистики выполните следующие действия:

1. Нажмите на значок ⚙ (**Настроить информационную панель**).
2. В разделе **Показывать статистику** выберите **Все**, **TCP** или **Поиск через API**.

   По умолчанию выбран вариант **Все**.

> Получение статистики по данным, получаемым через общедоступные API с помощью методов поиска, требует дополнительных вычислительных ресурсов. Чтобы избежать снижения производительности, можно отредактировать раздел `<Source id="api_single_lookup">` конфигурационного файла `kl_feed_service.conf` и изменить регулярные выражения на `(.*)`. Это, однако, может привести к неправильному расчету статистики.

Просмотр статистики в полноэкранном режиме

Статистику работы Kaspersky CyberTrace можно просматривать в полноэкранном режиме.

Чтобы просмотреть статистику в полноэкранном режиме,

нажмите на кнопку **Перейти в полноэкранный режим**.

Чтобы выйти из полноэкранного режима,

нажмите кнопку **Выйти из полноэкранного режима** либо нажмите клавишу **Esc**.

Отображение и скрытие виджета

Показывать и скрывать каждый из виджетов можно независимо от остальных.

Чтобы показать или скрыть виджет:

Нажмите на строку с названием виджета.

Если виджет показан, рядом с его именем отображается значок ⌄; если виджет скрыт, рядом с его именем отображается значок ›.

Скрытие и отображение виджетов

Включать и выключать отображение виджетов на информационной панели можно как в режиме **Управление системой**, так и в режиме **Управление данными**.

Чтобы показать или скрыть виджет, выполните следующие действия:

1. Нажмите на значок ⚙ (**Настроить информационную панель**).
2. В разделе **Виджеты** установите флажки для виджетов, которые требуется отображать на информационной панели, либо снимите флажки для виджетов, которые требуется скрыть.

   Чтобы скрыть или показать все виджеты, установите или снимите флажок **Скрыть все**.
3. Нажмите на кнопку **Сохранить**.

   Настройки виджетов сохраняются отдельно для каждого пользователя в режимах **Управление системой** и **Управление данными**.

Виджет Обзор статистики

Этот виджет на странице **Информационная панель** отображает обзор статистики обнаружений киберугроз за указанный период. Виджет содержит следующие элементы:

- Диаграмма, показывающая общее количество входящих событий

  Эта диаграмма отображается, если выбран вариант **Входящие события**.

- Диаграмма, показывающая количество обнаруженных киберугроз

  На линейной диаграмме отображается статистика обнаруженных киберугроз по точкам. Отражаются киберугрозы за указанный период. Шкала времени разбита на часы, дни или недели, в зависимости от указанного периода.

  Эта диаграмма отображается, если выбран вариант **Количество обнаруженных киберугроз**.

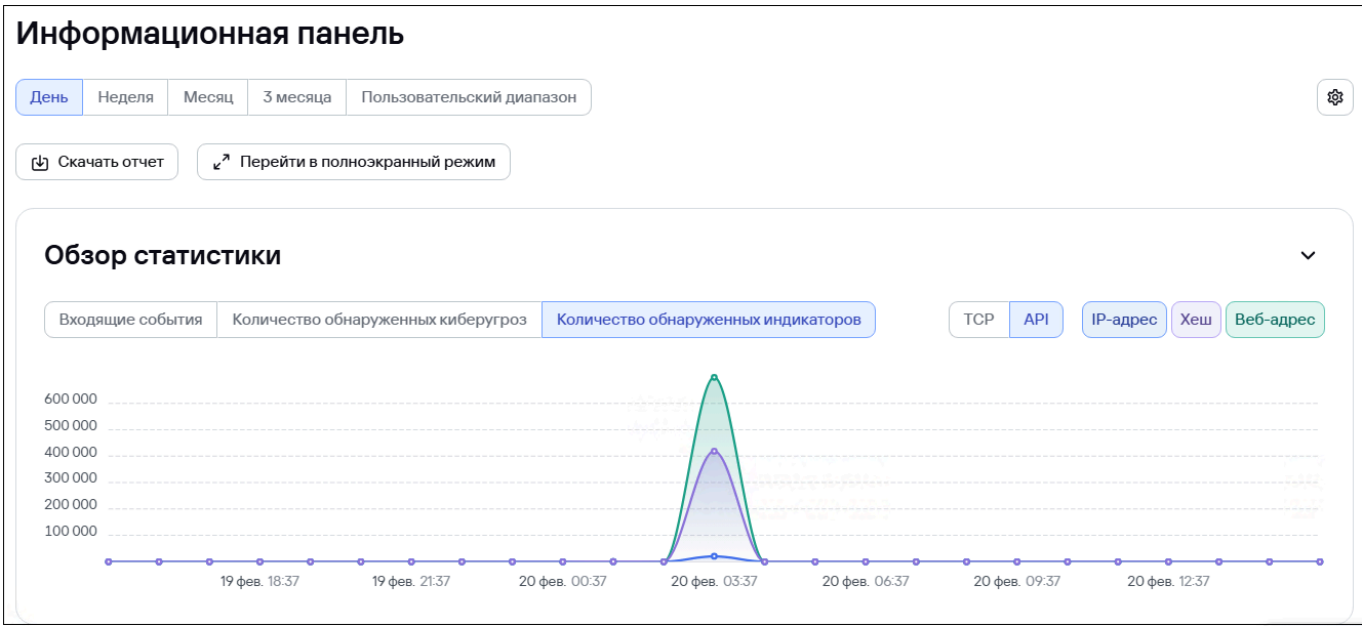
  В режиме **Управление данными** по нажатию на диаграмму в любой ее точке открывается страница **Обнаружения**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели.

- Диаграмма количества обнаруженных индикаторов для каждого типа индикатора (URL, IP-адрес, хеш)

  На линейной диаграмме отображается количество обнаруженных индикаторов за указанный период. Шкала времени разбита на часы, дни или недели, в зависимости от указанного периода.

  Эта диаграмма отображается, если выбран вариант **Количество обнаруженных индикаторов**.

В режиме **Управление данными** по нажатию на диаграмму или на тип индикатора открывается страница **Обнаружения**. На этой странице значения фильтруются по выбранному типу индикатора и периоду, указанному в настройках информационной панели.



Страница **Информационная панель**. Виджет **Обзор статистики**

При выборе произвольного диапазона для отображения данных на диаграммах виджета **Обзор статистики** могут использоваться различные временные интервалы, в зависимости от количества дней в выбранном периоде:

Выбранный диапазон	Временной интервал
От 1 до 48 часов	Часы
От 49 до 720 часов	Дни
Более 720 часов	Недели

При выборе периода, превышающего 720 часов (30 дней):

- Левая точка на диаграмме может не совпадать с датой начала выбранного периода, если количество дней в выбранном периоде не делится на 7.
- Значение крайней левой точки указывает на общее количество событий/обнаруженных киберугроз за предшествующие 7 дней.

Виджет «Топ обнаруженных индикаторов»

Этот виджет на странице **Информационная панель** отображает статистику обнаружений киберугроз за указанный период.

По нажатию на кнопку **Ретроскан** виджет выдает статистику обнаружений киберугроз, сделанных в результате ретроспективного сканирования.

По умолчанию этот виджет скрыт. Отображение виджета можно включить в настройках информационной панели. Это можно сделать только в режиме **Управление системой**.

Виджет содержит следующие элементы:

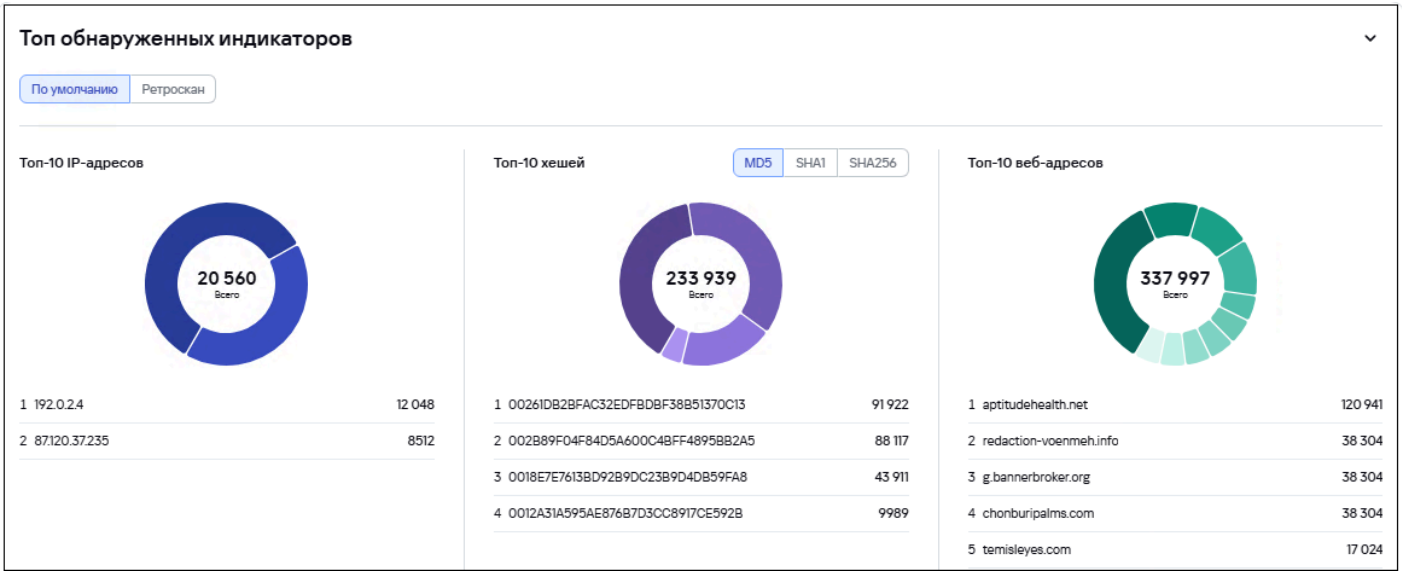
- Таблица с топ-10 обнаруженных IP-адресов с количеством обнаружений по каждому индикатору.
- Кольцевая диаграмма с относительными показателями обнаружения IP-адресов.

  При наведении указателя мыши на сегмент кольца отображается IP-адрес, количество обнаружений киберугроз для него и доля от общего числа обнаружений в процентах.
- Таблица с топ-10 обнаруженных хешей с количеством обнаружений по каждому индикатору (отдельно для хешей MD5, SHA1 и SHA256)
- Кольцевая диаграмма с относительными показателями обнаружения хешей (отдельно для хешей MD5, SHA1 и SHA256)

  При наведении указателя мыши на сегмент кольца отображается хеш, количество обнаружений киберугроз для него и доля от общего числа обнаружений в процентах.
- Таблица с топ-10 обнаруженных URL с количеством обнаружений по каждому индикатору.
- Кольцевая диаграмма с относительными показателями обнаружения URL.

  При наведении указателя мыши на сегмент кольца отображается URL, количество обнаружений киберугроз для него и доля от общего числа обнаружений в процентах.

В режиме **Управление данными** по нажатию на любой индикатор в таблице открывается страница **Сведения об индикаторе** и отображается подробная информация о выбранном индикаторе. По нажатию на количество обнаружений киберугроз для индикатора открывается страница **Обнаружения**. На этой странице значения фильтруются по выбранному индикатору.



Страница **Информационная панель**. Виджет **Топ обнаруженных индикаторов**

Виджет «Статистика сопоставлений»

Этот виджет на странице **Информационная панель** отображает статистику обнаружений киберугроз за указанный период. Виджет содержит следующие элементы:

- Бейдж с указанием общего количества проверенных индикаторов всех типов
- Бейдж с указанием общего количества обнаружений киберугроз для индикаторов всех типов

  В режиме **Управление данными** по нажатию на бейдж открывается страница **Обнаружения**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели.
- Бейдж с указанием общего количества индикаторов ложного срабатывания всех типов

  Этот бейдж отображается только в том случае, если в настройках информационной панели включено отображение ложных срабатываний.

  В режиме **Управление данными** по нажатию на бейдж открывается страница **Индикаторы**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели с включенным фильтром **Ложные срабатывания**.
- Таблица со статистикой проверенных индикаторов

  Таблица содержит следующие столбцы:

  - **Тип индикатора**

    Различные типы индикаторов.
  - **Проверено**

    Количество индикаторов каждого типа (URL, IP-адрес, хеш), которые проверяет служба Kaspersky CyberTrace.
  - **Обнаружено**

    Количество индикаторов каждого типа (URL, IP-адрес, хеш), обнаруженных службой Kaspersky CyberTrace.

    В режиме **Управление данными** по нажатию на значение в этом столбце открывается страница **Обнаружения**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели, и по выбранному типу индикатора.
  - **Ложные срабатывания**

    Количество ложных срабатываний каждого типа (URL, IP-адрес, хеш), обнаруженных службой Kaspersky CyberTrace.

    Этот столбец отображается только в том случае, если в настройках информационной панели включено отображение ложных срабатываний.

    В режиме **Управление данными** по нажатию на значение в этом столбце открывается страница **Индикаторы**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели, и по выбранному типу индикаторов, с включенным фильтром **Ложные срабатывания**.
- Кольцевая диаграмма, на которой отображается относительное количество проверенных индикаторов каждого типа (URL, IP-адрес, хеш)

  Эта кольцевая диаграмма отображается, если выбран вариант **Проверено**. При наведении указателя мыши на сегмент кольца отображается тип индикатора, количество индикаторов и процент от общего числа индикаторов.

- Кольцевая диаграмма, на которой отображается относительное количество обнаруженных индикаторов каждого типа (URL, IP-адрес, хеш)

  Эта кольцевая диаграмма отображается, если выбран вариант **Обнаружено**. При наведении указателя мыши на сегмент кольца отображается тип индикатора, количество индикаторов и процент от общего числа индикаторов.

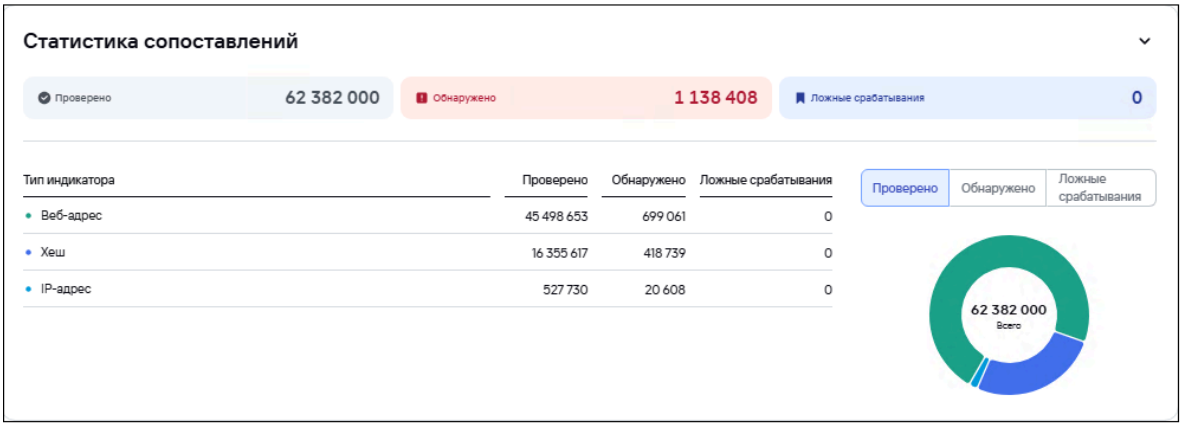
  В режиме **Управление данными** по нажатию на сегмент этой кольцевой диаграммы открывается страница **Обнаружения**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели, и по выбранному типу индикатора.

- Кольцевая диаграмма, на которой отображается относительное количество ложных срабатываний каждого типа (URL, IP-адрес, хеш)

  Эта кольцевая диаграмма отображается, если выбран вариант **Ложные срабатывания**. При наведении указателя мыши на сегмент кольца отображается тип индикатора, количество ложных срабатываний и процент от общего числа индикаторов.

  Эти кнопка и кольцевая диаграмма отображаются только в том случае, если в настройках информационной панели включено отображение ложных срабатываний.

  В режиме **Управление данными** по нажатию на сегмент этой кольцевой диаграммы открывается страница **Индикаторы**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели, и по выбранному типу индикаторов, с включенным фильтром **Ложные срабатывания**.



Страница **Информационная панель**. Виджет **Статистика сопоставлений**

Виджет «Статистика по потокам индикаторов»

Этот виджет отображается на странице **Информационная панель** и предоставляет статистические данные по обнаружениям киберугроз за указанный период, сгруппированные по источникам данных об угрозах. Виджет содержит следующие элементы:

- Бейдж с указанием общего количества индикаторов из всех источников данных об угрозах
- Бейдж с указанием общего количества обнаружений киберугроз для индикаторов из всех источников данных об угрозах

  В режиме **Управление данными** по нажатию на бейдж открывается страница **Обнаружения**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели.
- Бейдж с общим количеством обнаруженных индикаторов ложного срабатывания у всех источников данных об угрозах (индикаторы, принадлежащие источнику данных об угрозах *FalsePositive*)

  Этот бейдж отображается только в том случае, если в настройках информационной панели включено отображение ложных срабатываний.

  В режиме **Управление данными** по нажатию на бейдж открывается страница **Индикаторы**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели с включенным фильтром **Ложные срабатывания**.
- Таблица со статистикой обнаруженных киберугроз для каждого используемого источника данных об угрозах

  Таблица содержит следующие столбцы:

  - **Название потока индикаторов**

    Название используемого источника данных об угрозах.
  - Отметка ⚠ означает, что источник данных об угрозах не загружен или частично загружен из-за ограничений, накладываемых сертификатом, или что источник данных об угрозах отключен в настройке потоков данных. Кроме того, название такого источника данных об угрозах отображается светло-серым цветом.
  - **Дата обновления**

    Дата и время последнего обновления источника данных об угрозах.

    Если при попытке обновления источника данных об угрозах возникнет ошибка, Kaspersky CyberTrace отобразит уведомление об этом.
  - **Индикаторы**

    Количество индикаторов в источнике данных об угрозах.

    В режиме **Управление данными** по нажатию на значение в этом столбце открывается страница **Индикаторы**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели, и по выбранному источнику данных об угрозах.
  - **Обнаружено**

    Количество обнаружений индикаторов для каждого источника данных об угрозах.

    В режиме **Управление данными** по нажатию на значение в этом столбце открывается страница **Обнаружения**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели, и по выбранному источнику данных об угрозах.
  - **Ложные срабатывания**

Количество обнаружений индикаторов ложного срабатывания у каждого источника данных об угрозах (индикаторы, принадлежащие источнику данных об угрозах *FalsePositive*).

Этот столбец отображается только в том случае, если в настройках информационной панели включено отображение ложных срабатываний.

В режиме **Управление данными** по нажатию на значение в этом столбце открывается страница **Индикаторы**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели, и по выбранному источнику данных об угрозах, с включенным фильтром **Ложные срабатывания**.

- Кольцевая диаграмма, показывающая количество индикаторов для каждого используемого источника данных об угрозах

  Эта кольцевая диаграмма отображается, если выбран вариант **Индикаторы**. При наведении указателя мыши на сегмент кольца отображается тип источника данных об угрозах, количество индикаторов и процент от общего числа.

  В режиме **Управление данными** по нажатию на сегмент этой кольцевой диаграммы открывается страница **Индикаторы**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели, и по выбранному источнику данных об угрозах.

- Кольцевая диаграмма, показывающая количество обнаружений киберугроз для каждого используемого источника данных об угрозах

  Эта кольцевая диаграмма отображается, если выбран вариант **Обнаружено**. При наведении указателя мыши на сегмент кольца отображается тип источника данных об угрозах, количество обнаружений и процент от общего числа.

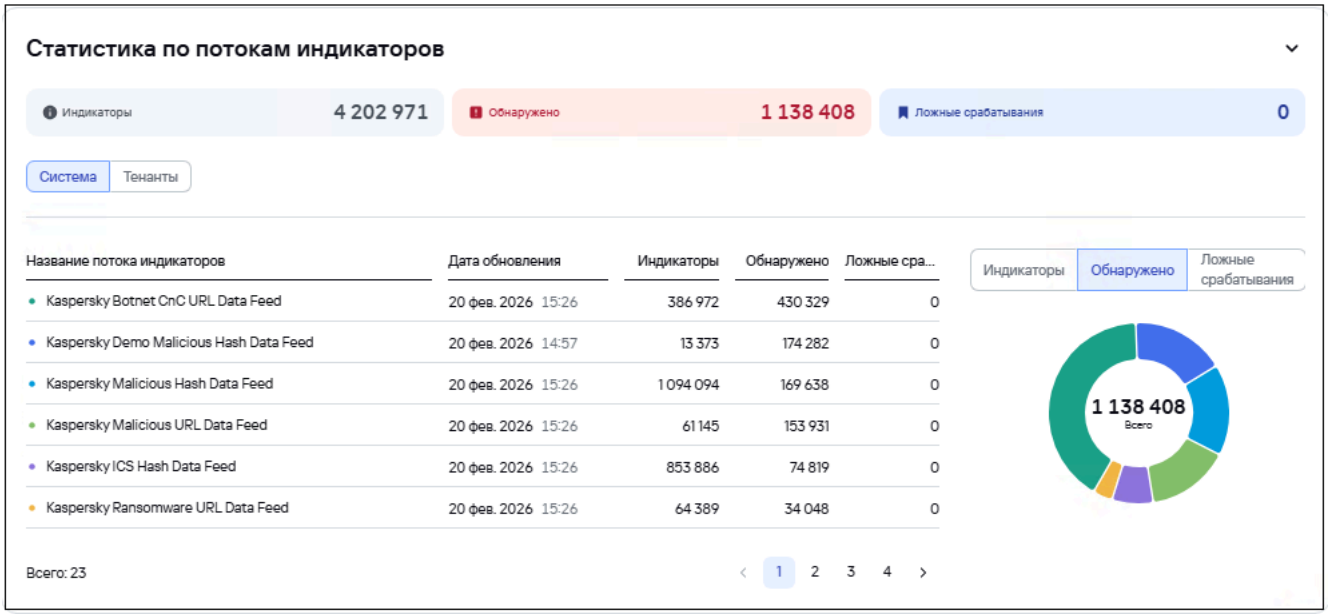
  В режиме **Управление данными** по нажатию на сегмент этой кольцевой диаграммы открывается страница **Обнаружения**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели, и по выбранному источнику данных об угрозах.

- Кольцевая диаграмма, показывающая количество индикаторов ложного срабатывания в (индикаторов, принадлежащих источнику данных об угрозах *FalsePositive*) для каждого используемого источнику данных об угрозах

  Эта кольцевая диаграмма отображается, если выбран вариант **Ложные срабатывания**. При наведении указателя мыши на сегмент кольца отображается тип источника данных об угрозах, количество индикаторов ложного срабатывания и процент от общего числа индикаторов.

  Эти кнопка и кольцевая диаграмма отображаются только в том случае, если в настройках информационной панели включено отображение ложных срабатываний.

В режиме **Управление данными** по нажатию на сегмент этой кольцевой диаграммы открывается страница **Индикаторы**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели, и по выбранному источнику данных об угрозах, с включенным фильтром **Ложные срабатывания**.



Страница **Информационная панель**. Виджет **Статистика по потокам индикаторов**

Если в списке ложных срабатываний есть записи, в таблице будет содержаться строка, в которой указано **Kaspersky FalsePositive** в столбце **Название потока индикаторов** и размер списка ложных срабатываний в столбце **Индикаторы**. В остальных столбцах в этой строке указано **0**.

Если в списке пользовательских сведений о киберугрозах есть записи, в таблице будет строка, в которой указано **Kaspersky InternalTI** в столбце **Название потока индикаторов** и размер списка пользовательских сведений о киберугрозах в столбце **Индикаторы**. В столбце **Обнаружено** в этой строке указано количество обнаруженных киберугроз по списку пользовательских сведений о киберугрозах, а в столбце **Ложные срабатывания** указано значение **0**.

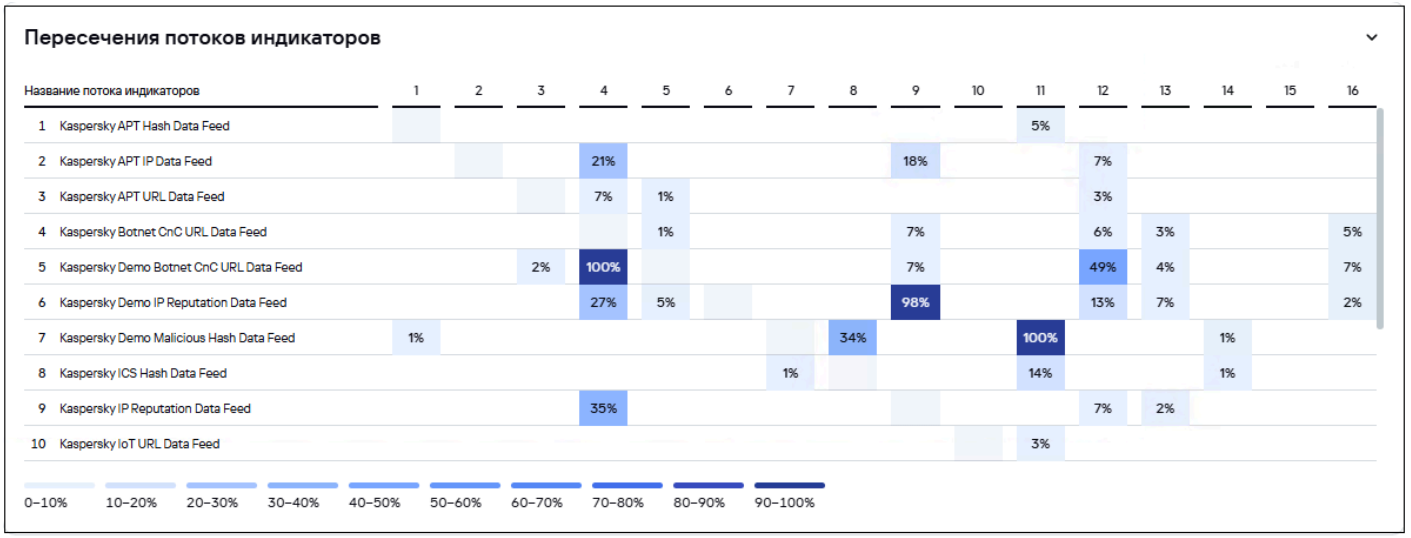
Виджет «Пересечения потоков индикаторов»

Этот виджет отображается на странице **Информационная панель** и показывает процент взаимопересечения источников данных об угрозах, используемых в Kaspersky CyberTrace. При переключении в режим **Управление данными** в таблице отображается пересечение источников данных об угрозах, используемых в этом тенанте.

Таблица состоит из строк и столбцов с источниками данных об угрозах Пересечение показывает, какой процент индикаторов из источников данных об угрозах в строках также присутствует в источниках данных об угрозах в столбцах.

В режиме **Управление данными** по нажатию на ненулевое значение в пересечении двух источников данных об угрозах открывается страница **Индикаторы**. На этой странице значения фильтруются по выбранному источнику данных об угрозах.

На этом виджете не отображаются источники данных об угрозах *FalsePositive* и *InternalTI*, а также источники данных об угрозах, не содержащие индикаторов.



Страница **Информационная панель**. Виджет **Пересечения потоков индикаторов**

Добавление пользовательских виджетов

На странице **Информационная панель** веб-интерфейса Kaspersky CyberTrace можно добавлять пользовательские виджеты. На этих виджетах отображается статистика обнаружений киберугроз для выбранных индикаторов.

Для работы с этой функцией необходимо перейти в режим **Управление данными**.

По умолчанию эта функция отключена. Эту функцию можно включить в настройках панели управления. Это можно сделать только в режиме **Управление системой**.

Можно добавить два пользовательских виджета:

- Один экземпляр виджета **Статистика обнаружений**.
- Один экземпляр виджета **Статистика обнаружений ретроскана**.

Для этих виджетов можно выбрать различные наборы индикаторов.

Виджет **Статистика обнаружений**

Этот виджет предоставляет статистику обнаружений киберугрозы для выбранных индикаторов. Виджет содержит следующие элементы:

- Бейдж с указанием общего количества обнаружений киберугроз для выбранных индикаторов

  При нажатии на бейдж открывается страница **Обнаружения**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели. Список обнаружений киберугроз можно дополнительно отфильтровать путем ввода значения индикатора в строку поиска.

- Бейдж с указанием общего количества индикаторов ложного срабатывания среди выбранных индикаторов

Этот бейдж отображается только в том случае, если в настройках информационной панели включено отображение ложных срабатываний.

При нажатии на бейдж открывается страница **Индикаторы**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели с включенным фильтром **Ложные срабатывания**.

- Таблица со статистикой обнаружений киберугроз по выбранным индикаторам

  Таблица содержит следующие столбцы:

  - **Тип**

    Тип индикатора.

  - **Индикатор**

    Значение индикатора.

  - **Обнаружено**

    Количество обнаруженных киберугроз по этому индикатору.

    По нажатию значение в этом столбце открывается страница **Обнаружения**. На этой странице значения фильтруются по периоду, указанному в настройках информационной панели, и по выбранному индикатору.

  - **Ложные срабатывания**

    Значок (серый флаг), указывающий на то, что индикатор был отмечен как ложное срабатывание.

    Этот столбец отображается только в том случае, если в настройках информационной панели включено отображение ложных срабатываний.

Виджет **Статистика обнаружений ретроскана**

Этот виджет предоставляет статистику обнаружений, сделанных в результате ретроспективного сканирования, для выбранных индикаторов. Виджет содержит те же элементы, что и виджет **Статистика обнаружений**.

По нажатию на бейдж с общим количеством обнаружений или на значение в столбце **Обнаружено**, значения на открывшейся странице **Обнаружения** отображаются с включенным дополнительным фильтром **Ретроскан**.

Добавление пользовательского виджета

Чтобы добавить пользовательский виджет, выполните следующие действия:

1. Нажмите на кнопку **Добавить виджет**.

   Если оба пользовательских виджета уже добавлены, эта кнопка становится недоступной.

2. В открывшемся окне **Добавление виджета** выберите тип виджета.

   Если виджет определенного типа уже добавлен, выбрать его еще раз невозможно.

3. Нажмите кнопку + (плюс) рядом с индикаторами, которые требуется добавить на виджет.

   Для каждого виджета можно выбрать до 50 индикаторов.

4. Нажмите на кнопку **Добавить**.

   Виджет добавляется на информационную панель

Изменение пользовательского виджета

Чтобы изменить пользовательский виджет, выполните следующие действия:

1. В разделе соответствующего виджета нажмите на кнопку **Изменить**.
2. В открывшемся окне **Изменение виджета** измените набор индикаторов для виджета. Для этого нажмите кнопку + (плюс) рядом с индикаторами, которые требуется добавить, и нажмите кнопку ✓ (галочка) рядом с индикаторами, которые требуется убрать.
3. Нажмите на кнопку **Сохранить**.

   Виджет изменен.

Удаление пользовательского виджета

Чтобы удалить пользовательский виджет, выполните следующие действия:

1. В разделе соответствующего виджета нажмите на кнопку **Удалить**.
2. В открывшемся окне подтверждения нажмите кнопку **Удалить**.

   Виджет удален. В случае необходимости можно будет снова добавить виджет того же типа.

Скачивание статистического отчета

Вы можете настроить и загрузить отчеты по статистике в формате PDF в разделе **Информационная панель**. При необходимости вы можете настроить рассылку отчетов в формате PDF по электронной почте.

Чтобы загрузить статистические отчеты в разделе **Информационная панель**, у вас должен быть один из следующих уровней лицензирования: Community Edition, Matching Engine, TIP Enterprise.

Чтобы скачать отчет, убедитесь, что в операционной системе Linux установлены следующие библиотеки: glibc версии 2.28 или более поздней, libstdc++ версии 6.0.25 или более поздней.

Чтобы загрузить отчет в формате PDF, выполните следующие действия:

1. На странице **Информационная панель** нажмите кнопку **Скачать отчет**.
2. В открывшемся окне **Скачать отчет** настройте отчет:
   - **Свойства отчета**:
     - **Источник данных**

       В качестве источника данных можно выбрать **TCP**, **Поиск через API** или **Все**.
     - **Период с**

       В этом поле укажите период отображения статистики.
     - **Тенанты**

       В этом поле укажите тенантов, данные которых будут включены в отчет. Тенанты можно выбирать только в режиме **Управление системой**. В режиме **Управление данными** в отчет включаются только данные того тенанта, в котором выполняется задача.
     - **Язык**

       В этом поле выберите язык отчета. По умолчанию используется язык, настроенный в вашей учетной записи.
     - Если требуется включить в отчет ложные срабатывания, установите соответствующий флажок.
   - **Свойства страницы**

     В отчет можно добавить титульную страницу, логотип «Лаборатории Касперского», логин и Ф.И.О. пользователя, установив соответствующие флажки.
   - **Виджеты**

     Выберите виджеты, которые требуется включить в отчет.

     Для виджета **Обзор статистики** можно установить следующие флажки:
     - **Входящие события**
     - **Количество обнаруженных киберугроз**
     - **Количество обнаруженных индикаторов**

     Для виджета **Топ обнаруженных индикаторов** можно установить следующие флажки:
     - **По умолчанию**
     - **Ретроскан**
     - **Топ-10 хешей**: MD5, SHA1, SHA256
3. Нажмите на кнопку **Download**.

Отчет в формате PDF скачивается.

Поиск индикаторов

В веб-интерфейсе Kaspersky CyberTrace на странице **Поиск** можно выполнять поиск индикаторов угроз. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Из-за ограничений, налагаемых уровнем лицензирования, эта функция может быть отключена.

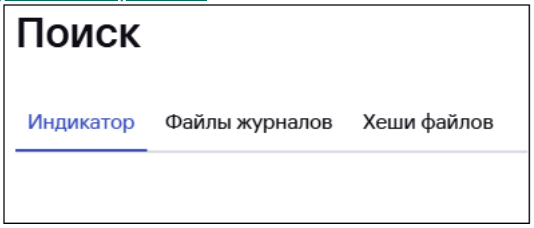
На странице **Поиск** можно работать со вкладками для отдельных типов поиска:

- **Индикатор**. Поиск указанного индикатора.

  Эта вкладка открыта по умолчанию.

- **Файлы журналов**. Поиск индикаторов из загруженных файлов журналов.

- **Хеши файлов**. Поиск хешей загруженных файлов.



Страница **Поиск**

Все поисковые запросы добавляются в историю поисковых запросов.

Сохранение результатов поиска

Результаты поиска можно сохранить в текстовый файл.

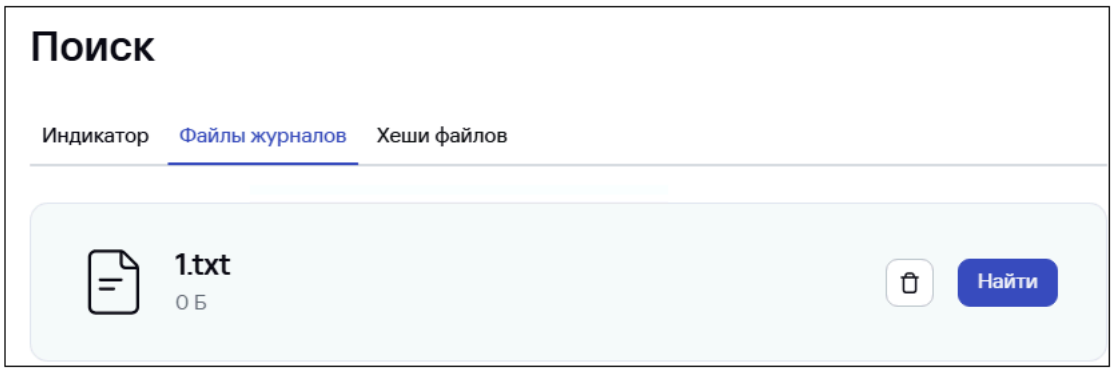
Результат будет сохранен в файле с именем `kl_lookup_result_%TYPE%_hhmmss_ddMMyyyy.txt`. Вместо `%TYPE%` подставляется либо `indicator` (для поиска по отдельному индикатору), либо `logfiles` (для поиска файлов журнала), либо `files` (для поиска хешей файлов).

Полный отчет о результатах поиска указан в файле CSV. В первой строке этого файла приводятся имена полей. Остальные строки отчета содержат значения полей, заключенные в кавычки. Если значение поля содержит знак кавычки, добавляется вторая кавычка. Все данные разделены точками с запятой.

Разные типы поиска подразумевают разные наборы полей в файле отчета. Наборы полей для каждого типа поиска описаны в разделе, посвященном соответствующему типу поиска.

Отмена поиска

Операцию поиска можно отменить.



Кнопка **Отмена**

Чтобы отменить операцию поиска, выполните следующие действия:

Нажмите на кнопку **Отмена** в правой части экрана.

Если операция поиска отменяется, результат поиска добавляется в историю поисковых запросов с результатом поиска **Отменено**. Форма результатов поиска очищается. Информация об обработанном элементе добавляется в историю поисковых запросов с пометкой о том, что процесс поиска не был завершен.

О синтаксисе поиска индикаторов

В этом разделе перечислены типы индикаторов, которые можно искать, и соответствующий синтаксис поискового запроса.

URL

Для поиска доменных имен и определенных URL используется следующий синтаксис:

- Доменные имена второго уровня
  `example.com`
- Доменные имена третьего и уровня и ниже
  `www.example.com`
- URL
  `http://www.example.com/index.html`

Хеши

Для поиска хешей используется следующий синтаксис:

- MD5
  `1A79A4D60DE6718E8E5B326E338AE533`
- SHA1
  `C3499C2729730A7F807EFB8676A92DCB6F8A3F8F`
- SHA256
  `50D858E0985ECC7F60418AAF0CC5AB587F42C2570A884095A9E8CCACD0F6545C`

IP-адреса

Для поиска адресов IPv4 используется следующий синтаксис:

`198.51.100.0`

Поиск IP-адресов, представленных в нотации бесклассовой междоменной маршрутизации (CIDR), не поддерживается.

Об истории поисковых запросов

В этом разделе описывается история поисковых запросов, которая отображается на каждой странице поиска угроз.

Хранение поисковых запросов

Информация о поисковых запросах, выполненных в веб-интерфейсе Kaspersky CyberTrace, сохраняется в истории. При выполнении поиска по файлу журнала сам файл журнала не хранится, сохраняются только те строки из файла журнала, которые содержали обнаруженные индикаторы; кроме того, при выполнении поиска по хешу сами файлы также не сохраняются.

Для каждого аутентифицированного пользователя HTTP-служба Kaspersky CyberTrace хранит следующий объем информации:

- Последние 1000 запросов на поиск индикаторов за последние три месяца.
- Последние 1000 запросов на поиск файлов за последние три месяца.
- Последние 1000 запросов на поиск хешей файлов за последние три месяца.

Отображение истории поисковых запросов

На каждой странице поиска имеется форма с историей запросов. Форма истории запросов содержит поисковые запросы соответствующего типа:

- Запрос поиска по отдельному индикатору
- Запрос поиска в файлах журналов
- Запрос поиска по хешу файла

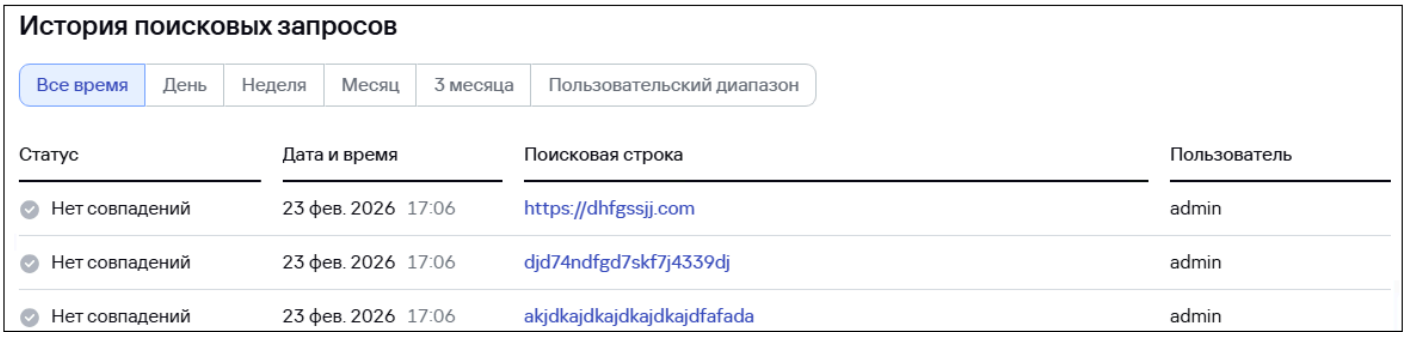
Администраторам доступна история поисковых запросов всех пользователей; остальным пользователям доступна только собственная история поисковых запросов.

Отображаемые поисковые запросы сортируются от последнего к первому. На активной странице содержится до 20 поисковых запросов. При наличии более 20 поисковых запросов следующие из них можно отобразить с помощью элементов управления навигацией.

Можно указать период, за который требуется отобразить поисковые запросы:

- Прошедшие сутки
- Последняя неделя
- Месяц (30 дней)
- 3 месяца (91 день)
- Произвольный период

История поисковых запросов по отдельному индикатору



История поисковых запросов по отдельному индикатору

На форме с историей поисковых запросов по отдельному индикатору отображаются следующие данные:

- Результат поиска

  Результат поиска **Найдено совпадение** означает, что индикатор был обнаружен один или несколько раз, **Нет совпадений** означает, что индикатор не был обнаружен, а **Отменено** означает, что операция поиска была отменена.

  Эта информация отображается в столбце **Статус**.

- Дата поискового запроса

  Например, 22 окт. 2024 17:20.

Эта информация отображается в столбце **Дата и время**.

- Индикатор, поиск которого выполнялся

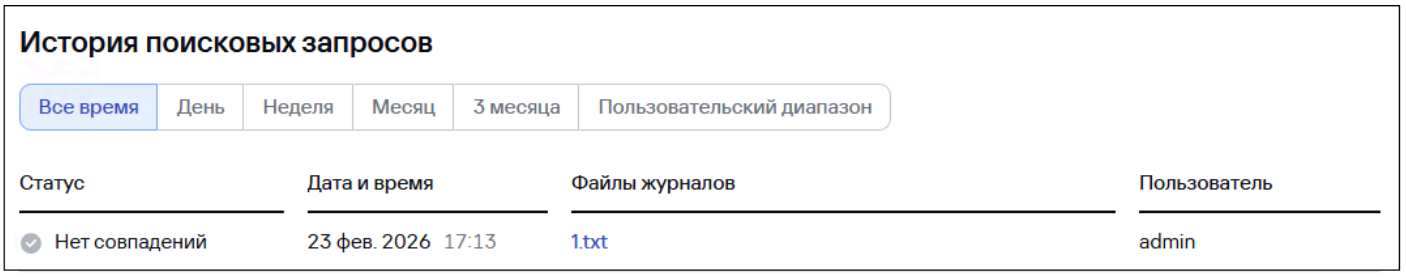
  Эта информация отображается в столбце **Поисковая строка**.

- Имя пользователя, выполнившего поисковый запрос

  Эта информация отображается в столбце **Пользователь** и доступна только администраторам.

Для не отмененной операции поиска при выборе индикатора отображается полный результат поиска и кнопка экспорта результата поиска.

История запросов поиска в файлах журналов



История запросов поиска в файлах журналов

На форме с историей поисковых запросов в файлах журналов отображаются следующие данные:

- Результат поиска

  Результат поиска **Найдено совпадение** означает, что индикаторы в файлах журналов были обнаружены один или несколько раз, **Нет совпадений** означает, что индикаторов обнаружено не было, а **Отменено** означает, что операция поиска была отменена.

  Эта информация отображается в столбце **Статус**.

- Дата поискового запроса

  Например, 22 окт. 2024 17:20.

  Эта информация отображается в столбце **Дата и время**.

- Файлы журналов, в которых выполнялся поиск индикаторов

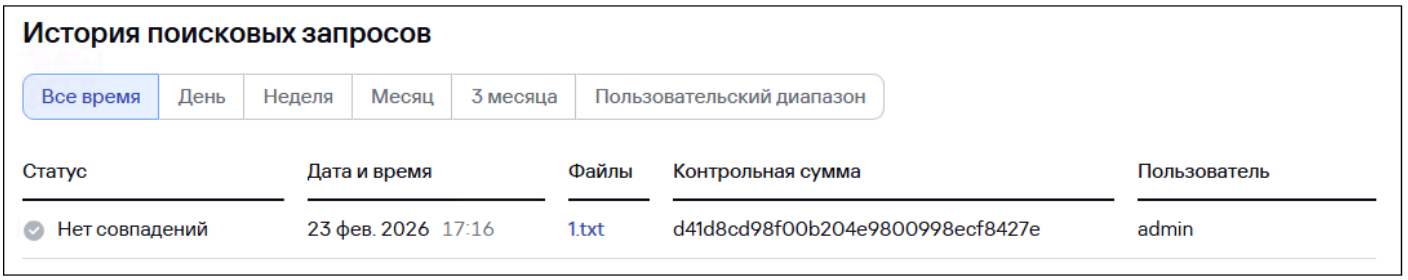
  Эта информация отображается в столбце **Файлы журналов**.

- Имя пользователя, выполнившего поисковый запрос

  Эта информация отображается в столбце **Пользователь** и доступна только администраторам.

Для не отмененной операции поиска при выборе строки в таблице отображается полный результат поиска и кнопка экспорта результата поиска.

История запросов поиска по хешу файла



История запросов поиска по хешу файла

На форме с историей поисковых запросов по хешу файла отображаются следующие данные:

- Результат поиска

  Результат поиска **Найдено совпадение** означает, что хеш файла был обнаружен один или несколько раз, **Нет совпадений** означает, что хеш файла не был обнаружен, а **Отменено** означает, что операция поиска была отменена.

  Эта информация отображается в столбце **Статус**.

- Дата поискового запроса

  Например, 22 окт. 2024 17:20.

  Эта информация отображается в столбце **Дата и время**.

- Имя файла, поиск хеша которого выполнялся

  Эта информация отображается в столбце **Файлы**.

- Хеш файла, поиск которого выполнялся

  Эта информация отображается в столбце **Контрольная сумма**.

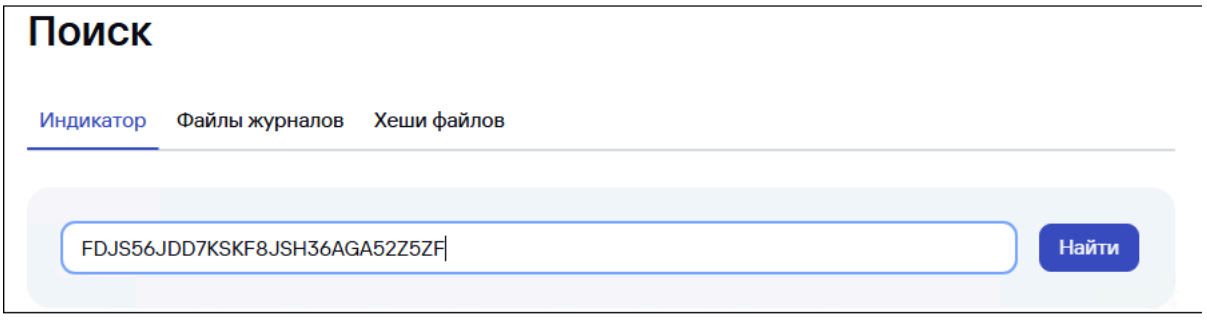
- Имя пользователя, выполнившего поисковый запрос

  Эта информация отображается в столбце **Пользователь** и доступна только администраторам.

Для не отмененной операции поиска при выборе хеша файла отображается полный результат поиска и кнопка экспорта результата поиска.

Поиск по отдельному индикатору

Для поиска по отдельному индикатору необходимо перейти на вкладку **Индикатор** на странице **Поиск**. Для работы с этой страницей необходимо перейти в режим **Управление данными**.



Вкладка **Индикатор**

Поиск объектов

Можно выполнять поиск индикаторов следующих типов:

- Hash
- IP Address
- URL

Чтобы выполнить поиск индикатора, выполните следующие действия:

1. Введите индикатор в поле поиска.
2. Нажмите на кнопку **Найти**.

Результат поиска отображается в разделе **Результаты поиска**.

Синтаксис поиска индикаторов

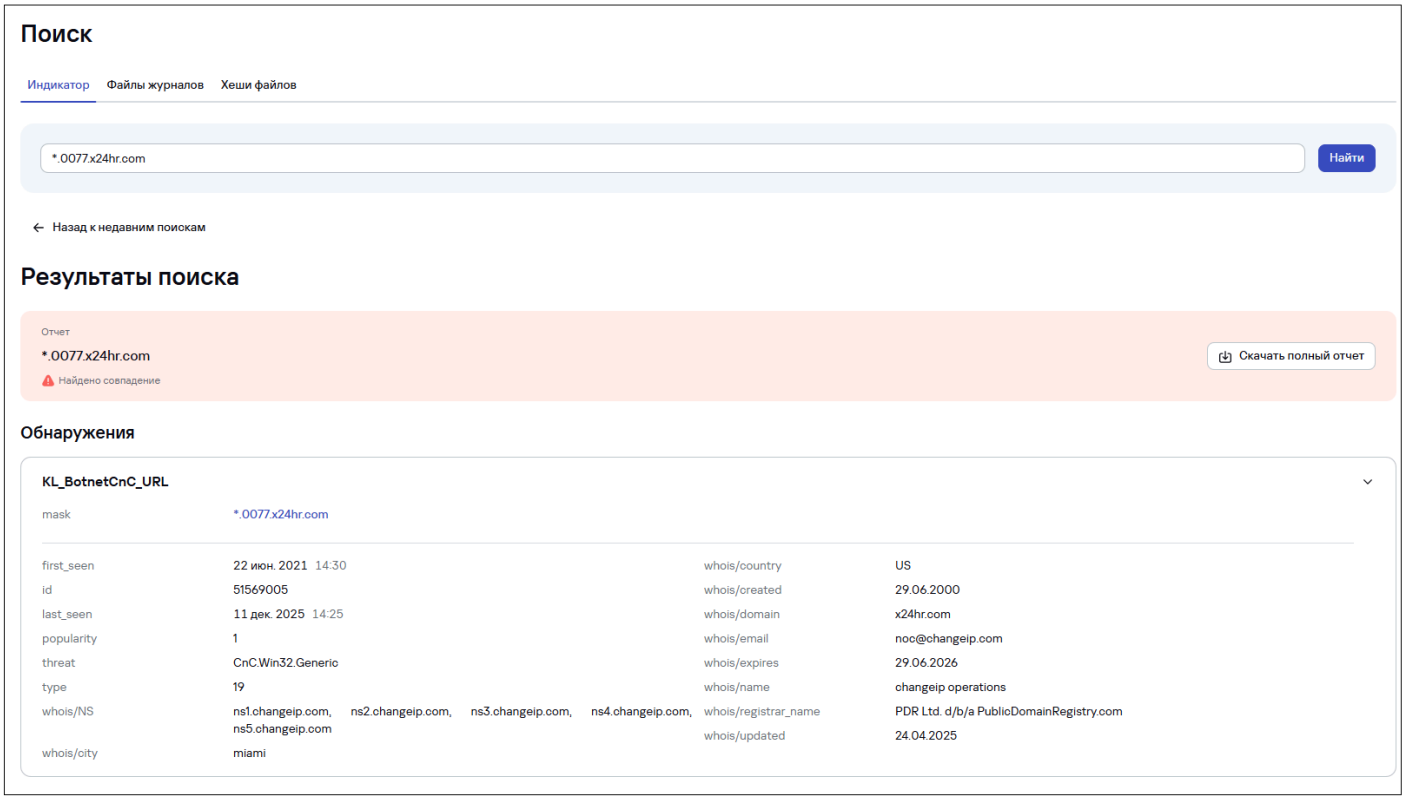
Поиск URL можно выполнить двумя способами:

- Путем указания полного URL
- Путем указания только доменного имени

При поиске хеша или IP-адреса необходимо указывать полный индикатор, как описано в разделе о синтаксисе поиска индикаторов.

Результат поиска

После выполнения поиска результаты отображаются в веб-интерфейсе Kaspersky CyberTrace в разделе **Результаты поиска**.



Раздел **Результаты поиска**

Результат поиска включает в себя следующие данные:

- Запрашиваемый индикатор
- Категория запрашиваемого индикатора
- Поля записей потока данных об угрозах, совпавших с индикатором

  Если в потоках данных об угрозах отсутствует информация о запрошенном индикаторе, отображается сообщение об этом.
- Ссылка или ссылки на подробную информацию о запрашиваемом индикаторе
- Кнопка для загрузки отчета о результатах поиска

Если индикатор не обнаружен, поскольку он принадлежит источнику данных об угрозах *FalsePositive*, в результатах поиска отображается сообщение о том, что подходящие индикаторы не найдены, а также ссылка на страницу поиска Kaspersky Threat Intelligence Portal.

Если после запуска поиска перейти на другую вкладку, результаты поиска добавляются в историю поисковых запросов.

Загрузка отчетов о поиске

Отчет с результатами операции поиска можно скачать. Отчет представляет собой файл .csv.

Чтобы скачать отчет, выполните следующие действия:

Нажмите на кнопку **Скачать полный отчет** и в случае запроса укажите каталог, в который требуется сохранить отчет.

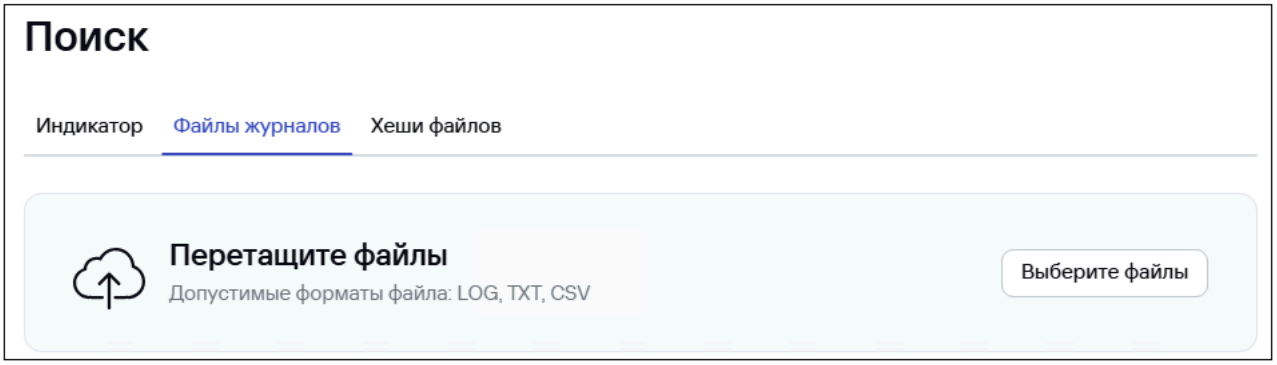
Регулярные выражения для поиска индикаторов

Для поиска индикаторов в веб-интерфейсе Kaspersky CyberTrace используются регулярные выражения, определенные в конфигурационном файле Kaspersky CyberTrace Service. Регулярные выражения задаются специальным источником событий с именем `http_single_lookup`.

Поиск индикаторов в файлах журналов

Для поиска индикаторов в файлах журналов необходимо выбрать вкладку **Файлы журналов** на странице **Поиск**. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Все файлы журналов, передаваемые в Kaspersky CyberTrace для проверки, должны быть в кодировке UTF-8. Если файлы журналов имеют другую кодировку, их необходимо преобразовать в UTF-8.



Вкладка **Файлы журналов**

Поиск объектов

Можно указать один или несколько файлов журналов. Поиск выполняется по индикаторам, входящим в эти файлы.

Для поиска индикаторов в файлах журналов выполните следующие действия:

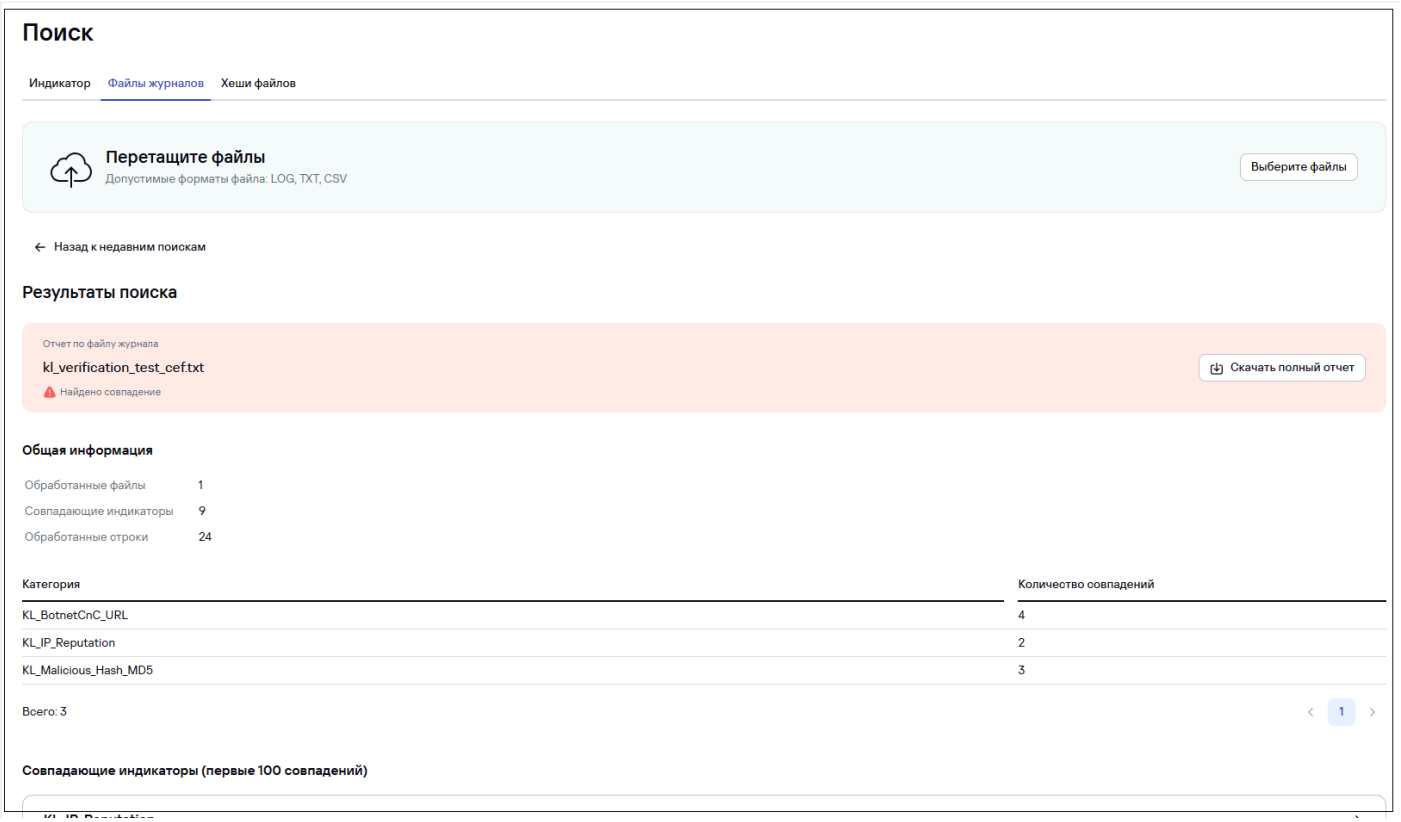
1. Выберите файлы журналов, в которых требуется выполнить поиск. Выполните одно из следующих действий:
   - Нажмите на кнопку **Выберите файлы**, затем выберите файлы журналов.
   - Перетащите файлы журналов в цветную область.
2. Нажмите на кнопку **Найти**.

Результат поиска отображается в разделе **Результаты поиска**.

Не следует использовать потоки данных об угрозах в качестве файлов журналов для поиска. Результаты проверки будут содержать большое количество совпадений, что сделает результаты неинформативными.

Результат поиска

После выполнения поиска результаты отображаются в веб-интерфейсе Kaspersky CyberTrace в разделе **Результаты поиска**.



Раздел **Результаты поиска**

Результат поиска включает в себя следующие данные:

- Сводная информация о результатах поиска:
  - Количество обработанных файлов журналов
  - Количество совпавших индикаторов
  - Количество обработанных строк
  - Количество совпадений по каждой категории
- Информация о топ-100 совпавших индикаторах
- Кнопка для загрузки отчета о результатах поиска

По каждой позиции из топ-100 совпавших индикаторов отображается следующая информация:

- Категория совпавшего индикатора
- Поля записей потока данных об угрозах, совпавших с индикатором
- Имя файла журналов и строки, содержащие обнаруженный индикатор

  Обнаруженный индикатор снабжается гиперссылкой на подробную информацию о нем.

Если информация об индикаторах не найдена в файле журнала, отображается сообщение об этом.

Если после запуска поиска перейти на другую вкладку, результаты поиска добавляются в историю поисковых запросов.

Загрузка отчетов о поиске

Отчет с результатами операции поиска можно скачать. Отчет представляет собой файл .csv.

Чтобы скачать отчет, выполните следующие действия:

Нажмите на кнопку **Скачать полный отчет** и в случае запроса укажите каталог, в который требуется сохранить отчет.

Полный отчет о результатах поиска содержит следующие поля:

- `file_name` — имя файла журнала
- `file_line` — строка в файле журнала, содержащая совпавший индикатор
- `detected_indicator` — совпавший индикатор
- `category` — категория совпавшего индикатора
- Поля контекста из потока данных об угрозах

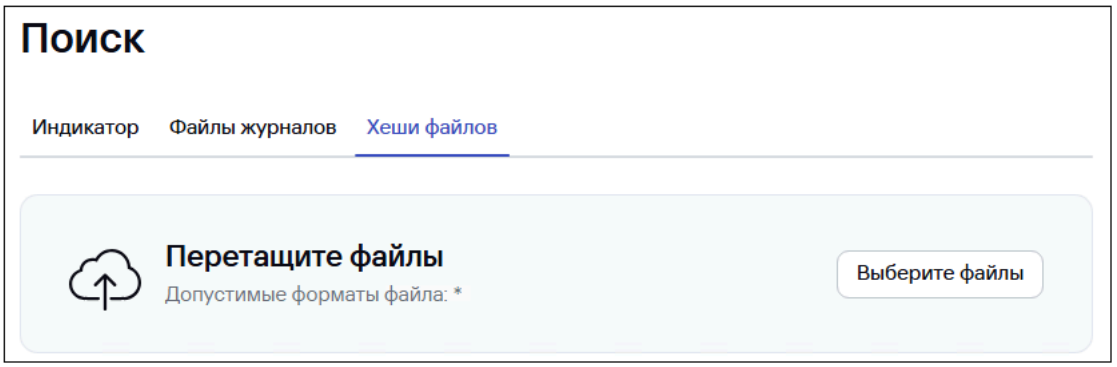
Файлы с отчетами о поиске хранятся в каталоге `httpsrv`. Открывать этот каталог имеет право только администратор (в Windows) или пользователь root (в Linux).

Регулярные выражения для поиска индикаторов в файлах журналов

Для парсинга файлов журналов для поиска индикаторов в веб-интерфейсе Kaspersky CyberTrace используются регулярные выражения, определенные в конфигурационном файле Kaspersky CyberTrace Service. Регулярные выражения задаются специальным источником событий с именем `http_file_lookup`.

Поиск хешей файлов

Для поиска хешей файлов необходимо перейти на вкладку **Хеши файлов** на странице **Поиск**. Для работы с этой страницей необходимо перейти в режим **Управление данными**.



Вкладка **Хеши файлов**

Поиск объектов

Можно указать один или несколько файлов. Поиск выполняется по MD5-хешам, входящим в эти файлы.

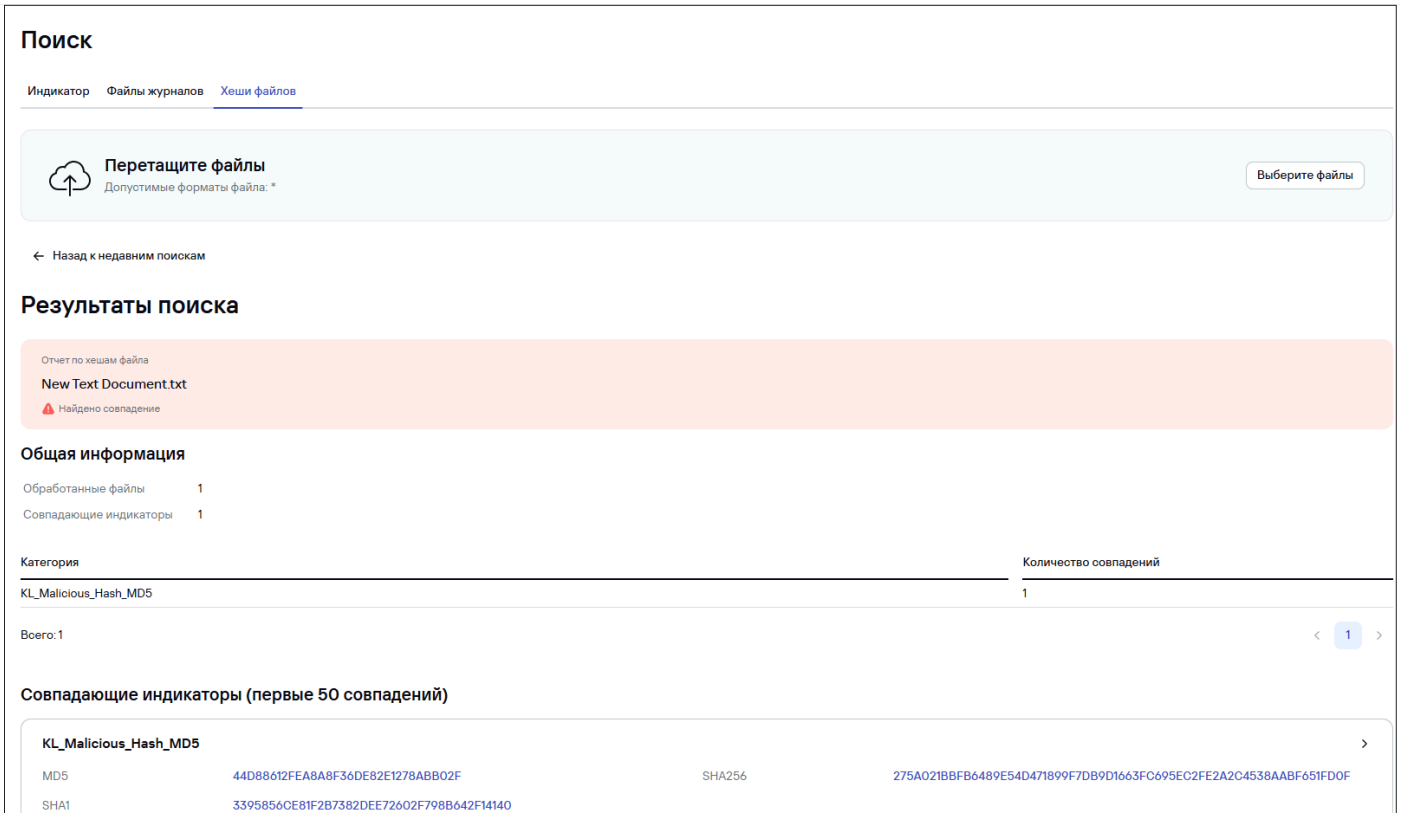
Для поиска хешей файлов выполните следующие действия:

1. Выберите файлы, поиск которых требуется выполнить. Выполните одно из следующих действий:
   - Нажмите на кнопку **Выберите файлы**, затем выберите файлы.
   - Перетащите файлы в цветную область.
2. Нажмите на кнопку **Найти**.

Результат поиска отображается ниже, в разделе **Результаты поиска**.

Результат поиска

После выполнения поиска результаты отображаются в веб-интерфейсе Kaspersky CyberTrace в разделе **Результаты поиска**.



Раздел **Результаты поиска**

Результат поиска включает в себя следующие данные:

- Количество обработанных файлов
- Количество совпавших индикаторов
- Количество совпадений по каждой категории

Для каждого проверенного хеша файла отображается следующая информация:

- Имя файла
- Хеш файла MD5

  Хеш файла снабжается ссылкой на подробную информацию об объекте.
- Поля записей потока данных об угрозах, сопоставленных с индикатором

Если информация по запрашиваемому файлу не найдена, выводится сообщение об этом.

Если после запуска поиска перейти на другую вкладку, результаты поиска добавляются в историю поисковых запросов.

Загрузка отчетов о поиске

Отчет с результатами операции поиска можно скачать. Отчет представляет собой файл .csv.

Чтобы скачать отчет, выполните следующие действия:

Нажмите на кнопку **Скачать полный отчет** и в случае запроса укажите каталог, в который требуется сохранить отчет.

Полный отчет о результатах поиска содержит следующие поля:

- `file_name` — имя файла, хеш которого обнаружен;
- `detected_indicator` — обнаруженный хеш;
- `category` — категория обнаруженного хеша;
- Поля контекста из потока данных об угрозах.

Просмотр результатов ретроспективного сканирования

В веб-интерфейсе Kaspersky CyberTrace можно выбрать страницу **Ретроскан**. Для работы с этим разделом необходимо перейти в режим **Управление системой**. Этот режим доступен только пользователям с ролью «Администратор».

Перед использованием ретроспективного сканирования его необходимо включить и настроить. В дальнейшем параметры ретроспективного сканирования также можно будет изменять.

Ретроспективное сканирование позволяет повторно проверять входящие события с объектами (IP-адрес, домен, URL или хеш), которые ранее не были признаны вредоносными. Причиной проверки результатов могло быть отсутствие в Kaspersky CyberTrace информации о связанных угрозах на момент получения этих объектов. Однако, поскольку потоки данных об угрозах постоянно обновляются, может быть полезно сохранять события, не содержащие обнаруженных индикаторов, а затем использовать обновленный список индикаторов, чтобы повторно проверять эти события вручную или по расписанию.

Обнаружения ретроспективного сканирования включаются в статистику и отображаются на странице **Обнаружения**, а также на графе, как и все обычные обнаружения. Результаты ретроспективного сканирования отправляются в SIEM-систему. Так же, как и в случае обычных обнаружений, применяются фильтры для отправки обнаружений ретроспективного сканирования в SIEM.

Когда выполняется ретроспективное сканирование, все неконтекстные значения, полученные из событий путем применения регулярных выражений, указанных в настройках ретроспективного сканирования на вкладке **Регулярные выражения**, сопоставляются с новыми индикаторами потоков данных об угрозах, включенных на вкладке **Потоки данных**.

Для редактирования или добавления новых регулярных выражений перейдите на страницу **Параметры** → **Источники событий**. Сохраненные регулярные выражения будут доступны в параметрах ретроспективного сканирования на вкладке **Регулярные выражения**.

В случае обнаружения киберугрозы события, отображенные в Kaspersky CyberTrace после добавления индикатора в поток данных об угрозах, будут отображаться на странице **Обнаружения** и не будут подвергаться ретроспективному сканированию.

Если индикатор был добавлен в поток данных об угрозах после получения его хеша, IP- или URL-адреса во время ретроспективного сканирования с помощью регулярного выражения и при отсутствии обнаружений, связанных с этим индикатором, то при следующем ретроспективном сканировании информация об этом индикаторе будет отображаться в столбце **Обнаруженные индикаторы**, а в столбце **Дата и время** будут отображаться дата и время обнаружения индикатора во время ретроспективного сканирования.

Для каждого события, связанного с этим индикатором, будет создана отдельная запись в отчете о ретроспективном сканировании.

Страница **Ретроскан** позволяет запустить ретроспективное сканирование вручную и просмотреть результаты, после завершения процесса сканирования.

На этой странице можно выполнить следующие действия:

- Запуск ретроспективного сканирования вручную
- Настройка отображения результатов проверки
- Просмотр подробной информации об отдельном результате ретроспективного сканирования, содержащем обнаруженные индикаторы

На этой странице также отображается следующее:

- Дата и время следующей задачи ретроспективного сканирования
- Количество событий, сохраненных для ретроспективного сканирования
- Размер событий, сохраненных для ретроспективного сканирования

  > Размер событий отображается с задержкой до одного часа. Фактический текущий размер сохраненных событий может быть больше отображаемого значения.

- Таблица с результатами ретроспективного сканирования за указанный период

  Таблица содержит следующие столбцы:

  - Статус задачи ретроспективного сканирования:

    - **Обнаружено**

      Результат содержит обнаруженные индикаторы.

    - **Не обнаружено**

      Результат не содержит обнаруженных индикаторов.

    - **Отменено**

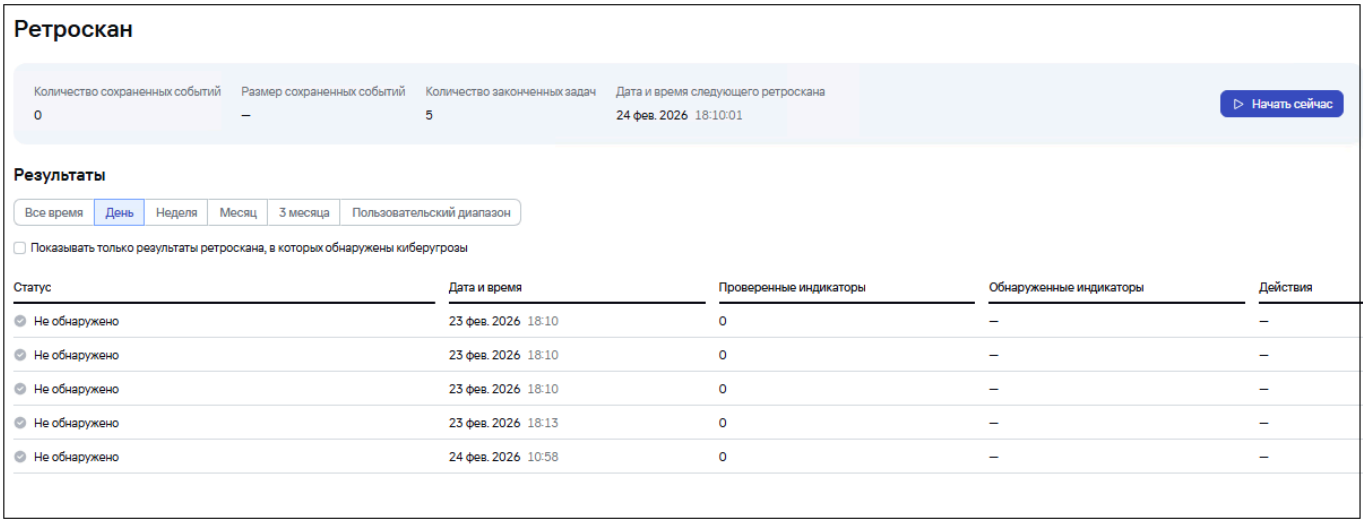
      Процесс ретроспективного сканирования был отменен.

    - **Ошибка**

      Сбой процесса ретроспективного сканирования.

  - Дата и время завершения каждой задачи ретроспективного сканирования

- Количество проверенных индикаторов
- Количество обнаруженных индикаторов



Результаты ретроспективного сканирования

Запуск ретроспективного сканирования

Чтобы запустить ретроспективное сканирование, выполните следующие действия:

Нажмите на кнопку **Начать сейчас**.

При необходимости процесс сканирования можно отменить.

Запуск ретроспективного сканирования может быть недоступен по нескольким причинам:

- Kaspersky CyberTrace в данный момент выполняет другую задачу ретроспективного сканирования.
- Ретроспективное сканирование отключено.

Настройка отображения результатов ретроспективного сканирования, содержащих оповещения об обнаружении индикаторов компрометации

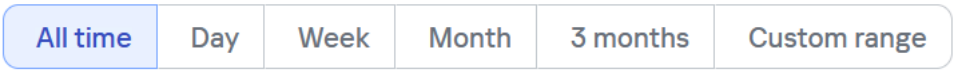
Чтобы отобразить только результаты, содержащие оповещения об обнаружении индикаторов компрометации, выполните следующие действия:

Установите флажок **Показывать только результаты ретроскана, в которых обнаружены киберугрозы** над таблицей **Результаты**.

Указание периода отображения результатов

Чтобы указать период времени для отображения результатов, можно выбрать один из вариантов над таблицей **Результаты**. Можно выбрать один из следующих периодов:

- **Все время**
- **День**
- **Неделя**
- **Месяц**
- **3 месяца**
- **Пользовательский диапазон**



Указание периода времени для результатов ретроспективного сканирования

Просмотр результатов отдельной задачи ретроспективного сканирования

Чтобы просмотреть подробную информацию об отдельной задаче ретроспективного сканирования:

1. В таблице **Результаты** найдите результат (содержащий обнаруженные индикаторы), подробности о котором требуется просмотреть.
2. Нажмите на ссылку **Подробнее**.

> На открывшейся странице приводится подробная информация о первых 50 событиях обнаруженных киберугроз. Чтобы просмотреть все события, скачайте полный отчет в формате CSV (см. ниже).

На странице отображается следующая информация:

- Дата и время ретроспективного сканирования

  > Дата и время, отображаемые на странице результатов сканирования, могут отличаться от даты и времени, указанных в отчете в формате CSV. Это связано с настройками времени в формате UTC: в отчете в формате CSV всегда используется часовой пояс UTC+0, а время на странице результатов сканирования зависит от пользовательских настроек.

- Количество обработанных событий
- Количество обнаруженных индикаторов
- Количество обработанных индикаторов

- Количество оповещений об обнаружении индикаторов компрометации по категориям
- Информация о каждом событии обнаружения киберугроз в разделе **Обнаруженные индикаторы**

  Чтобы просмотреть подробную информацию о каждом индикаторе, можно развернуть панель с соответствующим индикатором. Эта информация содержится в следующих полях:

  - Категория обнаруженного объекта
  - **Метка времени** — дата и время обнаружения индикатора
  - **Тенант** — имя тенанта, связанное с исходным событием
  - **Источник** — источник события, отправивший исходное событие
  - **ioc** — поле, по которому обнаружен индикатор
  - **IP** — поле, полученное с помощью регулярного выражения

Загрузка отчета с результатами ретроспективного сканирования

Чтобы скачать отчет, выполните следующие действия:

Нажмите на кнопку **Скачать полный отчет**.

Сгенерированный файл CSV содержит следующие данные:

- Дата и время получения оповещения об обнаружении индикаторов компрометации

  > Дата и время, отображаемые на странице результатов сканирования, могут отличаться от даты и времени, указанных в отчете в формате CSV. Это связано с настройками времени в формате UTC: в отчете в формате CSV всегда используется часовой пояс UTC+0, а время на странице результатов сканирования зависит от пользовательских настроек.

- Имя тенанта, связанное с исходным событием
- Имя источника событий
- Категория обнаруженного объекта
- Обнаруженный индикатор, вызвавший событие
- Контекстная информация об оповещении об обнаружении индикаторов компрометации
- Оповещение об обнаружении индикаторов компрометации

Просмотр обнаруженных киберугроз

На странице **Обнаружения** веб-интерфейса Kaspersky CyberTrace отображается информация о входящих событиях, которые привели к возникновению обнаруженных киберугроз в Kaspersky CyberTrace, в том числе источники событий и оповещения об обнаружении индикаторов компрометации. На этой странице можно выполнять поиск событий и фильтрацию событий по критериям. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Страница **Обнаружения** содержит следующие элементы:

- Панель поиска
- Таблица с информацией об обнаруженных киберугрозах
- Кнопка перехода к настройкам таблицы:
  - Переключатель **Искать также в оповещениях об обнаружении индикаторов компрометации**
  - Переключатель **Автоматически обновлять таблицу**
  - **Столбцы таблицы**
- Кнопка для экспорта обнаружений киберугроз в файл CSV

Поиск по обнаруженным киберугрозам

С помощью строки поиска можно выполнять полнотекстовый поиск по обнаруженным киберугрозам. Текстовая строка в поисковом запросе токенизируется таким образом, чтобы результаты поиска содержали как точные, так и нечеткие совпадения. Подстановочные знаки не поддерживаются.

Результаты поиска отображаются в таблице ниже.

Если включен переключатель **Искать также в оповещениях об обнаружении индикаторов компрометации**, Kaspersky CyberTrace будет искать текстовую строку во входящих событиях и оповещениях об обнаружении индикаторов компрометации. В противном случае поиск выполняется только по входящим событиям. По умолчанию переключатель **Искать также в оповещениях об обнаружении индикаторов компрометации** выключен.

Таблица с информацией об обнаруженных киберугрозах содержит следующие столбцы:

- **Дата обнаружения киберугрозы**

  Системные дата и время обнаружения киберугрозы.

- **Источник**

  Имя источника событий.

Этот столбец может содержать имя источника, которого уже нет в Kaspersky CyberTrace. Такая ситуация может возникнуть для обнаружения ретроспективного сканирования в том случае, если источник был удален или переименован после сохранения входящего события.

- **Категория**

  Категория обнаруженного объекта.

  Записанное имя категории не меняется, даже если изменится имя источника данных об угрозах.

- **Тип**

  Тип индикатора, на который сработало обнаружение киберугрозы.

- **Значение**

  Значение индикатора, на который сработало обнаружение киберугрозы.

- **Теги**

  Список тегов, присвоенных индикатору, на который сработало обнаружение киберугрозы.

- **Общий вес тегов**

  Суммарный вес тегов в столбце **Теги**.

- **Уровень доверия к потоку индикаторов**

  Уровень доверия к потоку данных или источнику данных об угрозах.

- **Дополнительная информация**:

  - **Источник**

    Показывает, получены ли обнаружения киберугроз через TCP (**TCP**), через публичный API (**API**) или обоими способами (**Все**).

    Значком API отмечаются обнаружения киберугроз, полученные через общедоступные API.

  - **Ретроскан**

    Показывает наличие или отсутствие обнаружений киберугроз в результате ретроспективного сканирования (**Ретроскан** или **Не ретроскан**) либо показывает все обнаружения (**Все**).

    Значок Retroscan указывает на наличие обнаружений киберугроз, полученных в результате ретроспективного сканирования.

  - **Ложн**

    Показывает, является ли обнаружение киберугрозы ложным срабатыванием (**Все**, **Ложные срабатывания** или **Не ложные срабатывания**).

    Значок (серый флаг), указывающий на то, что обнаружение киберугрозы, вместе с соответствующим индикатором, было отмечено как ложное срабатывание.

- Пользовательские столбцы

  Эти столбцы создаются в соответствии с регулярным выражениям источников событий тенанта и содержат индикаторы из источников событий, полученные с помощью регулярных выражений типа Context.

В каждой строке таблицы содержится информация об отдельной обнаруженной киберугрозе.

Обнаруженные киберугрозы в таблице сортируются по дате и времени в порядке убывания.

Если переключатель **Автоматически обновлять таблицу** включен, Kaspersky CyberTrace добавляет в таблицу новую информацию об обнаруженных киберугрозах каждые 10 секунд.

Настройка таблицы обнаружений киберугроз

Таблицу обнаружений киберугроз можно настраивать, скрывая или отображая отдельные столбцы.

Для настройки таблицы обнаружения киберугроз выполните следующие действия:

1. Нажмите на значок (**Параметры**).
2. В разделе **Столбцы таблицы** установите флажки для столбцов, которые должны отображаться в таблице обнаружений киберугроз, либо снимите флажки, чтобы скрыть соответствующие столбцы таблицы.
3. Нажмите на кнопку **Сохранить**.

Таблица обнаружения киберугроз настроена.

По умолчанию название пользовательского столбца, отображаемого в таблице, совпадает с названием соответствующего регулярного выражения. Если требуется изменить название пользовательского столбца, нажмите на значок (Изменить) и введите новое имя столбца.

Если источник событий или регулярное выражение были удалены или переименованы, а для соответствующего пользовательского столбца настроено отображение в таблице, такой пользовательский столбец отображается со значком , означающим, что регулярное выражение удалено.

Просмотр сведений об обнаружении киберугрозы

Нажатие на обнаружение киберугрозы позволяет просмотреть следующую подробную информацию:

- **Исходное событие**

  В этом разделе содержатся подстроки, извлеченные из входящего события с помощью регулярных выражений, а также исходное событие целиком.

- **Оповещение об обнаружении индикаторов компрометации**

  В этом разделе содержатся контекстные поля совпавшего индикатора в формате `%FieldName%=%Value%` и оповещение об обнаружении индикаторов компрометации целиком.

  где:

  - `%FieldName%` — это имя регулярного выражения, которое использовалось для парсинга входящего события, или имя поля записи потока данных об угрозах, которое было успешно сопоставлено с обнаруженным индикатором.
  - `%Value%` — это значение регулярного выражения, которое использовалось для парсинга входящего события, или значение записи потока данных об угрозах, успешно сопоставленное с обнаруженным индикатором.

Фильтрация обнаруженных киберугроз

Обнаруженные киберугрозы в таблице можно фильтровать по следующим критериям:

- **Дата обнаружения киберугрозы**

  Укажите период времени или конкретную дату.

- **Источник**

  Выберите один или несколько источников событий.

- **Категория**

  Выберите одну или несколько категорий обнаруженных объектов.

- **Уровень доверия к потоку индикаторов**

  Укажите интервал уровней доверия к потокам данных или источникам данных об угрозах.

- **Дополнительная информация**

  - **Источник**

    Выберите общедоступные API или TCP в качестве источника обнаружений киберугроз для отображения в таблице. Если фильтр не применен, отображаются все обнаружения киберугроз.

  - **Ретроскан**

    Выберите для отображения в таблице все обнаружения, обнаружения ретроспективного сканирования или обнаружения без ретроспективного сканирования. Если фильтр не применен, отображаются все обнаружения киберугроз.

  - **Ложн**

    Выберите, какие обнаружения киберугроз требуется отображать в таблице: отмеченные как ложные срабатывания или не отмеченные как ложные срабатывания. Если фильтр не применен, отображаются все обнаружения киберугроз.

Чтобы отфильтровать таблицу по критериям, выполните следующие действия:

1. Нажмите на значок ▽ (воронка) в столбце, который требуется использовать в качестве критерия фильтрации.

2. Укажите условие фильтрации.

3. Если в окне задания условия фильтрации есть кнопка **Применить**, нажмите ее.

Содержимое таблицы обновится и в нее будут включены только значения, соответствующие заданным условиям.

Можно указать несколько критериев фильтрации.

По умолчанию условия фильтрации не применяются.

Чтобы удалить фильтр, выполните следующие действия:

1. Нажмите на значок ▽ (воронка) в столбце, который требуется прекратить использовать в качестве критерия фильтрации.

2. Нажмите на кнопку **Сбросить**.

Содержимое таблицы обновится и больше не будет отфильтровано по удаленному критерию фильтрации.

О категориях обнаружений киберугроз

Ниже приведен список доступных категорий обнаружения. Эти категории применимы к потокам данных Kaspersky и OSINT, поддерживаемым Kaspersky CyberTrace.

Категория обнаружения киберугрозы	Описание
KL_APT_Hash_MD5	Kaspersky CyberTrace обнаруживает хеш вредоносного файла, используемого в APT-кампании.
KL_APT_Hash_SHA1	Kaspersky CyberTrace обнаруживает хеш вредоносного файла, используемого в APT-кампании.
KL_APT_Hash_SHA256	Kaspersky CyberTrace обнаруживает хеш вредоносного файла, используемого в APT-кампании.
KL_APT_IP	Kaspersky CyberTrace обнаруживает IP-адрес, используемый в APT-кампании.
KL_APT_URL	Kaspersky CyberTrace обнаруживает URL, используемый в APT-кампании.
KL_BotnetCnC_URL	Kaspersky CyberTrace обнаруживает URL командного сервера (C&C) ботнета.
KL_ICS_Hash_MD5	Kaspersky CyberTrace обнаруживает хеш ICS.
KL_ICS_Hash_SHA1	Kaspersky CyberTrace обнаруживает хеш ICS.
KL_ICS_Hash_SHA256	Kaspersky CyberTrace обнаруживает хеш ICS.
KL_InternalTI_URL	URL списка пользовательских сведений о киберугрозах Kaspersky CyberTrace.
KL_InternalTI_IP	IP-адрес списка пользовательских сведений о киберугрозах Kaspersky CyberTrace.
KL_InternalTI_Hash_MD5	Хеш списка пользовательских сведений о киберугрозах Kaspersky CyberTrace.
KL_InternalTI_Hash_SHA1	Хеш списка пользовательских сведений о киберугрозах Kaspersky CyberTrace.
KL_InternalTI_Hash_SHA256	Хеш списка пользовательских сведений о киберугрозах Kaspersky CyberTrace.
KL_IoT_Hash_MD5	Kaspersky CyberTrace обнаруживает хеш IoT.
KL_IoT_Hash_SHA1	Kaspersky CyberTrace обнаруживает хеш IoT.
KL_IoT_Hash_SHA256	Kaspersky CyberTrace обнаруживает хеш IoT.
KL_IoT_URL	Kaspersky CyberTrace обнаруживает URL, заражающий устройства с поддержкой интернета вещей (IoT).
KL_IP_Reputation	Kaspersky CyberTrace обнаруживает вредоносный IP-адрес.
KL_Malicious_URL	Kaspersky CyberTrace обнаруживает вредоносный URL.
KL_Malicious_Hash_MD5	Kaspersky CyberTrace обнаруживает вредоносный хеш.
KL_Malicious_Hash_SHA1	Kaspersky CyberTrace обнаруживает вредоносный хеш.
KL_Malicious_Hash_SHA256	Kaspersky CyberTrace обнаруживает вредоносный хеш.
KL_Mobile_Malicious_Hash_MD5	Kaspersky CyberTrace обнаруживает вредоносный мобильный хеш.
KL_Mobile_Malicious_Hash_SHA1	Kaspersky CyberTrace обнаруживает вредоносный мобильный хеш.
KL_Mobile_Malicious_Hash_SHA256	Kaspersky CyberTrace обнаруживает вредоносный мобильный хеш.
KL_Mobile_BotnetCnC_URL	Kaspersky CyberTrace обнаруживает URL командного сервера (C&C) мобильного ботнета.
KL_Phishing_URL	Kaspersky CyberTrace обнаруживает фишинговый URL.
KL_Ransomware_URL	Kaspersky CyberTrace обнаруживает URL, на котором размещена программа-вымогатель.

AbuseCh_Feodo_Block_IP	Kaspersky CyberTrace обнаруживает IP-адрес из потока данных об угрозах Abuse.Ch_Feodo_Block_IP.
AbuseCh_Ransomware_Block_URL	Kaspersky CyberTrace обнаруживает URL из потока данных об угрозах Abuse.Ch_Ransomware_Block_URL.
AbuseCh_Ransomware_Block_Domain	Kaspersky CyberTrace обнаруживает домен из потока данных об угрозах Abuse.Ch_Ransomware_Block_Domain.
AbuseCh_Ransomware_Block_IP	Kaspersky CyberTrace обнаруживает IP-адрес из потока данных об угрозах Abuse.Ch_Ransomware_Block_IP.
AbuseCh_Ransomware_Common_URL	Kaspersky CyberTrace обнаруживает URL из потока данных об угрозах Abuse.Ch_Ransomware_Common_URL.
AbuseCh_SSL_Certificate_Block_IP	Kaspersky CyberTrace обнаруживает IP-адрес из потока данных об угрозах AbuseCh_SSL_Certificate_Block_IP.
AbuseCh_SSL_Certificate_Hash_SHA1	Kaspersky CyberTrace обнаруживает хеш из потока данных об угрозах AbuseCh_SSL_Certificate_Hash_SHA1.
BlocklistDe_Block_IP	Kaspersky CyberTrace обнаруживает IP-адрес из потока данных об угрозах BlocklistDe_Block_IP.
CyberCrime_Tracker_Block_Url	Kaspersky CyberTrace обнаруживает URL из потока данных об угрозах CyberCrime_Tracker_Block_Url.
EmergingThreats_Block_IP	Kaspersky CyberTrace обнаруживает IP-адрес из потока данных об угрозах EmergingThreats_Block_IP.
EmergingThreats_Compromised_IP	Kaspersky CyberTrace обнаруживает IP-адрес из потока данных об угрозах EmergingThreats_Compromised_IP.

Экспорт обнаружений киберугроз в файл CSV

Вы можете экспортировать обнаружения киберугроз в файл CSV на странице **"Обнаружения киберугроз"**.

Файл CSV будет содержать обнаружения киберугроз, которые будут отображаться в таблице обнаружений киберугроз на момент экспорта.

Вы можете настроить отображаемые обнаружения киберугроз с помощью поиска обнаружений киберугроз, а также фильтрации и сортировки столбцов таблицы обнаружений киберугроз.

Чтобы экспортировать обнаружения киберугроз:

1. Перейдите в режим "Управление данными".
2. Перейдите на страницу **"Обнаружения киберугроз"**.
3. Нажмите на иконку (экспорт) над таблицей обнаружений киберугроз.

   Обнаружения киберугроз будут экспортированы в файл CSV.

Файл CSV соответствует следующим требованиям:

- Первая строка файла начинается с символа хеша (#), за которым следуют заголовки.
- Заголовки разделяются точкой с запятой (;).
- Значения разделяются точкой с запятой (;).
- Набор столбцов и их порядок соответствуют параметрам запроса.
- В файле будет указано не более 1000 обнаружений киберугроз.

- Имена заголовков в первой строке соответствуют именам столбцов таблицы обнаружения киберугроз в веб-интерфейсе.
- Имя файла имеет следующий формат: `Detections_%date%.csv`, где `%date%` – дата создания файла в формате ГГГГ-ММ-ДД.

Копирование данных обнаружения киберугрозы в буфер обмена

На странице `"Обнаружения киберугроз"` можно скопировать данные выбранных индикаторов в буфер обмена.

Чтобы скопировать данные обнаружения киберугрозы в буфер обмена:

1. Перейдите в режим "Управление данными".
2. Перейдите на страницу **"Обнаружения киберугроз"**.
3. Выберите обнаружение киберугрозы в таблице.
4. На странице **"Обнаружения киберугроз"** нажмите кнопку **"Копировать в буфер обмена"**.

   Данные обнаружения киберугрозы будут скопированы в буфер обмена.

Пример скопированных данных обнаружения киберугрозы выглядит следующим образом:

```
{
  "detections_details": {
    "detection_date": "2025-11-12T11:09:11Z",
    "source": "default",
    "category": "KL_Malicious_Hash_MD5",
    "hash": "44D88612FEA8A8F36DE82E1278ABB02F",
    "tags": [
      {
        "name": "MEDIUM_TAG",
        "weight": 3
      }
    ],
    "tagsWeight": 3,
    "confidence": 100,
    "additional_info": {
      "is_public_api": false,
      "is_retroscan": false,
      "is_false_positive": false
    }
  },
  "source_event": {
    "RE_HASH": [
      "44D88612FEA8A8F36DE82E1278ABB02F"
    ],
    "Device": [
      "Threat Feed Service"
    ],
    "Product": [
      "Threat Feed Service"
    ],
    "whole_source_event": "May 2 16:41:40 KL_Verification_Tool LEEF:1.0|Kaspersky Lab|Threat Feed
Service|4.0|KL_TEST_HASH|md5=44D88612FEA8A8F36DE82E1278ABB02F\tusrName=VerifTestUserName"
  },
  "detection_alert": {
    "MD5": "44D88612FEA8A8F36DE82E1278ABB02F",
    "SHA1": "3395856CE81F2B7382DEE72602F798B642F14140",
    "SHA256": "275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F",
    "file_size": 68,
    "first_seen": "02.04.2010 22:07",
    "id": -2,
    "last_seen": "12.11.2025 09:26",
    "popularity": 5,
    "threat": "EICAR-Test-File",
    "whole_detection_alert": "CEF:0|Kaspersky|Kaspersky CyberTrace for ArcSight|2.0|2|CyberTrace Detection
Event|8| reason=KL_Malicious_Hash_MD5 dst=- src=- fileHash=44D88612FEA8A8F36DE82E1278ABB02F request=-
sourceServiceName=Threat Feed Service sproc=Threat Feed Service suser=- msg=CyberTrace detected
KL_Malicious_Hash_MD5 externalId=-  flexString1=02.04.2010 22:07 flexString2=12.11.2025 09:26 cn2=5 cs3=EICAR-
Test-File cs4=- fsize=68 cs5Label=MatchedIndicator cs5=44D88612FEA8A8F36DE82E1278ABB02F cn3Label=Confidence
cn3=100 cs6Label=Context cs6=MD5:44D88612FEA8A8F36DE82E1278ABB02F SHA1:3395856CE81F2B7382DEE72602F798B642F14140
SHA256:275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F file_size:68 first_seen:02.04.2010 22:07
id:-2 last_seen:12.11.2025 09:26 popularity:5 threat:EICAR-Test-File "
  }
}
```


Все свойства, указанные в объекте `source_event`, за исключением `whole_source_event`, должны относиться к типу данных "массив". Свойство `all_source_event` должно относиться к строковому типу данных.

Об обнаружениях ретроспективного сканирования

Обнаружения, полученные в результате ретроспективного сканирования, имеют определенные отличия от обнаружений, полученных в результате сопоставления. В этом разделе описаны особенности обнаружений ретроспективного сканирования.

При ретроспективном сканировании входящее событие, сохраняемое для анализа в Kaspersky CyberTrace, отражает только значения, полученные с использованием регулярных выражений, указанных на вкладке **Регулярные выражения** настроек ретроспективного сканирования. Поэтому поле **Исходное событие целиком** на странице **Обнаружения** будет содержать местозаполнитель вместо входящего события.

Поле **EventReceivedDate** для обнаружений ретроспективного сканирования содержит дату получения исходного события, а не дату обнаружения, которая указана в столбце **Дата обнаружения киберугрозы**.

Если имена регулярных выражений были изменены в настройках в период с момента сохранения входящего события до момента формирования обнаружения ретроспективного сканирования, то контекст оповещения об обнаружении индикаторов компрометации, в котором используются измененные регулярные выражения, не будет включать соответствующие значения, так как в сохраненном событии они представлены под другими именами. См. пример ниже.

Входящее событие:

```
CEF:0|Kaspersky|CyberTrace Verification Kit|1.2|0|Verification_test|2| request=http://fakess123bn.nu
suser=EvalTestUserName src=192.168.0.0 dvc=127.0.0.0 dst=192.0.2.0 act=VerificationTest eventId=110
```

Настроенные регулярные выражения на момент получения события:

```
RE_URL: (?:\:\/\/)((?:\S+(?::\S*)?+@)?(?:(?:(?:[a-z\x{00a1}-\x{ffff}0-9]+-*)*[a-z\x{00a1}-\x{ffff}0-9]*)(?:\.(?:
[a-z\x{00a1}-\x{ffff}0-9]+-)*+[a-z\x{00a1}-\x{ffff}0-9]++)*(?:\.(?:[a-z\x{00a1}-\x{ffff}\-0-9]+)))(?:\.*:\d{2,5})?
+(?:\.*\/[^\s\"\<\>]*+)?+)

SRC_IP: (?:\:\/\/)((?:\S+(?::\S*)?+@)?(?:(?:(?:[a-z\x{00a1}-\x{ffff}0-9]+-*)*[a-z\x{00a1}-\x{ffff}0-9]*)(?:\.(?:
[a-z\x{00a1}-\x{ffff}0-9]+-)*+[a-z\x{00a1}-\x{ffff}0-9]++)*(?:\.(?:[a-z\x{00a1}-\x{ffff}\-0-9]+)))(?:\.*:\d{2,5})?
+(?:\.*\/[^\s\"\<\>]*+)?+)

UserName: suser\=(.*?)(?:$|\s)
```

Настроенные регулярные выражения на момент формирования обнаружения ретроспективного сканирования:

```
REGEX_URL: (?:\:\/\/)((?:\S+(?::\S*)?+@)?(?:(?:(?:[a-z\x{00a1}-\x{ffff}0-9]+-*)*[a-z\x{00a1}-\x{ffff}0-9]*)(?:\.
(?:[a-z\x{00a1}-\x{ffff}0-9]+-)*+[a-z\x{00a1}-\x{ffff}0-9]++)*(?:\.(?:[a-z\x{00a1}-\x{ffff}\-0-9]+)))
(?:\.*:\d{2,5})?+(?:\.*\/[^\s\"\<\>]*+)?+)

SRC_IP: (?:\:\/\/)((?:\S+(?::\S*)?+@)?(?:(?:(?:[a-z\x{00a1}-\x{ffff}0-9]+-*)*[a-z\x{00a1}-\x{ffff}0-9]*)(?:\.(?:
[a-z\x{00a1}-\x{ffff}0-9]+-)*+[a-z\x{00a1}-\x{ffff}0-9]++)*(?:\.(?:[a-z\x{00a1}-\x{ffff}\-0-9]+)))(?:\.*:\d{2,5})?
+(?:\.*\/[^\s\"\<\>]*+)?+)

USER_NAME: suser\=(.*?)(?:$|\s)
```

Формат обнаружения:

```
CEF:0|Kaspersky|Kaspersky CyberTrace for ArcSight|2.0|2|CyberTrace Detection Event|8| reason=%Category%
src=%SRC_IP% request=%REGEX_URL% suser=%USER_NAME% msg=CyberTrace detected %Category% cs5Label=MatchedIndicator
```

Сформированное обнаружение ретроспективного сканирования:

```
CEF:0|Kaspersky|Kaspersky CyberTrace for ArcSight|2.0|2|CyberTrace Detection Event|8| reason=KL_BotnetCnC_URL
src=192.168.0.0 request=- suser=- msg=CyberTrace detected KL_BotnetCnC_URL cs5Label=MatchedIndicator
cs5=fakess123bn.nu
```

Работа с индикаторами

Для хранения индикаторов компрометации (IOC) из потоков данных об угрозах Threat Intelligence в Kaspersky CyberTrace используется база данных Elasticsearch. Эта база данных входит в состав комплекта поставки Kaspersky CyberTrace.

В веб-интерфейсе Kaspersky CyberTrace можно перейти на страницу **Индикаторы**. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

На этой странице можно выполнять следующие действия:

- Просматривать список индикаторов из базы данных индикаторов (далее также именуется базой данных).
- Выполнять поиск по индикатору.
- Добавлять новые индикаторы в базу данных.

  Когда новый индикатор успешно добавляется в базу данных, его можно использовать в процессе сопоставления. Такие индикаторы записываются в базу данных с использованием значения *InternalTI* атрибута `supplier_name`.

- Удалять индикаторы из базы данных.
- Добавлять существующие индикаторы к источнику данных об угрозах *FalsePositive* (отмечать как ложное срабатывание).
- Просматривать подробную информацию об индикаторах.
- Фильтровать показатели по источникам данных об угрозах.

  При применении этого фильтра и выборе нескольких источников данных об угрозах Kaspersky CyberTrace показывает только те индикаторы, каждый из которых был предоставлен всеми выбранными источниками данных об угрозах.

- Фильтровать индикаторы по тегам.
- Фильтровать индикаторы по типу.

  Чтобы использовать этот фильтр, нажмите на заголовок столбца **Тип** и в открывшейся форме фильтра выберите типы индикаторов, которые должны отображаться в списке.

Источники данных об угрозах FalsePositive и InternalTI

Источники данных об угрозах *FalsePositive* и *InternalTI* представляют собой встроенные источники данных об угрозах Kaspersky CyberTrace, в которые можно добавлять индикаторы:

- Источник данных об угрозах *FalsePositive* предназначен для существующих индикаторов, которые пользователи отмечают как ложные срабатывания в веб-интерфейсе Kaspersky CyberTrace.
- Источник данных об угрозах *InternalTI* предназначен для новых индикаторов, которые пользователи добавляют в базу данных в веб-интерфейсе Kaspersky CyberTrace или через REST API.

Индикаторы источников данных об угрозах InternalTI будут срабатывать, даже если это индикатор из списка ложных срабатываний.

Просмотр индикаторов

На странице **Индикаторы** веб-интерфейса Kaspersky CyberTrace отображается таблица индикаторов компрометации. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Таблица с информацией об индикаторах состоит из следующих столбцов:

- **Тип**

  Тип индикатора. Индикатор может относиться к нескольким типам (например, IP и URL).

- **Значение**

  Значение индикатора.

- **Дата добавления**

  Дата и время, когда был добавлен индикатор.

- **Дата последнего обновления**

  Дата и время последнего обновления индикатора.

- **Теги**

  Список тегов, назначенных индикатору.

- **Общий вес тегов**

  Суммарный вес тегов в столбце **Теги**.

- **Потоки индикаторов**

  Источники данных об угрозах, содержащие индикатор.

- **Ложн**

  Значок (серый флаг), указывающий на то, что индикатор был отмечен как ложное срабатывание.

В таблице не отображаются индикаторы, которые содержатся только в списке ложных срабатываний (и не были добавлены в Kaspersky CyberTrace из потока данных, с помощью REST API или через веб-интерфейс Kaspersky CyberTrace). Можно отфильтровать только индикаторы из списка ложных срабатываний.

При поиске индикаторов в таблице отображаются только результаты поиска.

Под таблицей указано количество индикаторов, возвращенных после выполнения поиска. Без выполнения поиска отображается суммарное количество уникальных индикаторов для всех включенных источников данных об угрозах. Таблица не содержит повторяющихся значений индикаторов, а соответствующие источники данных об угрозах указываются в столбце **Потоки индикаторов**. Таким образом, дубликаты значений индикаторов исключаются из подсчета суммарного количества.

Индикаторы фильтрации

Индикаторы в таблице можно фильтровать по следующим критериям:

- **Тип**

  Выберите один или несколько типов индикаторов.

- **Общий вес тегов**

  Укажите диапазон суммарных весов тегов, присвоенных индикаторам.

- **Потоки индикаторов**

  Выберите источники данных об угрозах, содержащие индикаторы.

- **Ложн**

  Выберите, какие индикаторы требуется отображать в таблице: отмеченные как ложные срабатывания или не отмеченные как ложные срабатывания. Если фильтр не применен, отображаются все индикаторы.

Чтобы отфильтровать таблицу по критериям, выполните следующие действия:

1. Нажмите на значок (воронка) в столбце, который требуется использовать в качестве критерия фильтрации.

2. Укажите условие фильтрации.

3. Если в окне задания условия фильтрации есть кнопка **Применить**, нажмите ее.

Содержимое таблицы обновится и в нее будут включены только значения, соответствующие заданным условиям.

Можно указать несколько критериев фильтрации.

По умолчанию условия фильтрации не применяются.

Чтобы удалить фильтр, выполните следующие действия:

1. Нажмите на значок ▽ (воронка) в столбце, который требуется прекратить использовать в качестве критерия фильтрации.
2. Нажмите на кнопку **Сбросить**.

Содержимое таблицы обновится и больше не будет отфильтровано по удаленному критерию фильтрации.

Добавление индикаторов в список пользовательских сведений о киберугрозах

На странице **Индикаторы** можно добавить индикатор в список пользовательских сведений о киберугрозах с атрибутами или без них. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Чтобы добавить индикатор с атрибутами, выполните следующие действия:

1. Нажмите на кнопку **Добавить индикатор**.

   Откроется окно **Добавить индикатор**.
2. Выберите тип индикатора.
3. Укажите значение индикатора.

   > Kaspersky CyberTrace применяет правила нормализации URL ко всем добавляемым URL, которые еще не содержатся в базе данных индикаторов. Таким образом, представление того или иного URL может изменяться. Например, при добавлении URL, содержащего порт, значение порта удаляется.
4. Добавьте атрибуты индикатора путем указания их имен и значений.

   Имя может содержать до 255 символов, должно содержать только строчные латинские буквы и не может начинаться с дефиса («-») или знака подчеркивания («_»). Не допускаются символ пробела (« ») и символ табуляции. Кроме того, атрибут не может иметь имя `summary`.
5. При необходимости введите в текстовое поле сводную информацию об индикаторе.
6. Нажмите на кнопку **Добавить**.

Индикатор добавляется в базу данных, причем для атрибута `supplier_name` задается значение *InternalTI*.

Чтобы добавить один или несколько индикаторов без атрибутов, выполните следующие действия:

1. Нажмите на кнопку **Управлять пользовательским списком индикаторов**.
2. Выберите тип индикатора.

3. Каждое значение вводится с новой строки.

> Kaspersky CyberTrace применяет правила нормализации URL ко всем добавляемым URL, которые еще не содержатся в базе данных индикаторов. Таким образом, представление того или иного URL может изменяться. Например, при добавлении URL, содержащего порт, значение порта удаляется.

4. Нажмите на кнопку **Сохранить**.

Индикаторы добавляются в базу данных, причем для атрибута `supplier_name` задается значение *InternalTI*.

Проверка индикаторов IP, HASH, MD5, SHA1 и SHA256

Kaspersky CyberTrace проверит индикаторы IP, HASH, MD5, SHA1 и SHA256 при добавлении их в систему.

Если хотя бы один индикатор не пройдет проверку во время обновления задачи, то при наведении курсора на значок статуса задачи появится всплывающая подсказка с текстом в следующем формате:

- Название потока данных, индикаторы которого не прошли проверку.
- Количество индикаторов потока данных, не прошедших проверку.
- Общее количество индикаторов потока данных.

Удаление индикаторов

На странице **Индикаторы** можно удалить один или несколько индикаторов из базы данных. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Кроме того, отдельный индикатор можно удалить на странице с подробной информацией о нем.

> Удаление индикаторов доступно пользователям с ролью «Администратор».

Чтобы удалить индикатор, выполните следующие действия:

1. В таблице индикаторов установите флажки рядом с индикаторами, которые требуется удалить.
2. Нажмите на кнопку **Удалить**.
3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**, чтобы подтвердить удаление выбранных индикаторов.

Выбранные индикаторы удаляются из базы данных.

Поиск индикаторов в таблице индикаторов

На странице **Индикаторы** можно выполнять поиск индикаторов в базе данных. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Чтобы выполнить поиск индикаторов, выполните следующие действия:

1. В поле поиска укажите строку, которую требуется найти. Синтаксис поискового запроса описан далее в этом разделе.

   Длина поискового запроса – от 1 до 1024 символов Unicode.

2. Нажмите на кнопку **Найти**, чтобы начать поиск.

   На странице **Индикаторы** отобразится список индикаторов, совпавших с указанной строкой. Поисковый запрос можно сохранить, чтобы использовать его в будущем.

Синтаксис поисковых запросов

Строка поискового запроса для поиска по базе индикаторов должна следовать определенному синтаксису. Рассмотрим пример строки поискового запроса:

```
ioc_value: 192.0.2* OR (ioc_type: md5 AND ioc_updated_date:>=2020-01-01)
```

В строке поискового запроса можно использовать атрибуты со следующими именами:

Имя атрибута	Описание
`ioc_type`	Тип индикатора.
`ioc_value`	Значение индикатора.
`ioc_created_date`	Дата и время, когда запрошенный индикатор был добавлен в базу данных.
`ioc_updated_date`	Дата и время последнего обновления индикатора.
`ioc_comment`	Комментарий к индикатору.
`ioc_summary`	Сводная информация об индикаторе от источника данных об угрозах *InternalTI*.
`ioc_first_detected_date`	Дата и время, когда оповещение об обнаружении индикаторов компрометации в было впервые получено.
`ioc_last_detected_date`	Дата и время последнего получения оповещения об обнаружении индикаторов компрометации.
`username`	Имя пользователя, добавившего индикатор в источник данных об угрозах *InternalTI*/*FalsePositive*.
`ioc_supplier_can_match`	Флаг, показывающий, что индикатор может использоваться в процессе сопоставления. Этот флаг применяется к индикаторам, которые должны были быть удалены во время обновления источника данных об угрозах или по истечении срока хранения, но не были удалены, поскольку они принадлежат источнику данных об угрозах *InternalTI*, или поскольку такие индикаторы были задействованы в процессе обнаружения киберугроз. Этот параметр может принимать значения `true` или `false`.
`ioc_supplier_last_updated_date`	Дата и время последнего обновления информации об индикаторе от источника данных об угрозах.

`ioc_supplier_send_match_event`	Флаг отправки оповещений об обнаружении индикаторов компрометации в SIEM-систему.
`supplier_name`	Имя источника данных об угрозах, из которого был получен индикатор. В Kaspersky CyberTrace поддерживаются следующие типы источников данных об угрозах: • Загруженный файл потока данных об угрозах Для этого типа источника данных об угрозах в качестве значения атрибута `supplier_name` выступает имя файла потока данных об угрозах, указанного в kl_feed_util.conf. • Запрос REST API Для этого типа источника данных об угрозах значение атрибута `supplier_name` — это имя источника данных об угрозах, добавленного через REST API. • Пользовательский веб-интерфейс (источники данных об угрозах *InternalTI* и *FalsePositive*) Для этого типа источника данных об угрозах значение атрибута `supplier_name` зависит от списка, в добавляется индикатор (*InternalTI* или *FalsePositive*). Если вы новый индикатор добавляется на вкладке **Индикаторы** в веб-интерфейсе Kaspersky CyberTrace, используется значение *InternalTI*. Если вы индикатор добавляется в список ложных срабатываний в окне **Ложные срабатывания** на вкладке **Потоки данных** или если индикатор отмечается как ложное срабатывание, используется значение *FalsePositive*.
`supplier_confidence`	Уровень доверия к источнику данных об угрозах.
`supplier_vendor_name`	Имя поставщика источника данных об угрозах.
`ioc_supplier_context`	Контекстная информация, относящаяся к индикатору. Этот атрибут может содержать вложенные атрибуты. Правило для поиска всех вложенных атрибутов описано ниже.

Для поисковых запросов используется следующий синтаксис:

- Если в поисковом запросе для подстроки используются специальные символы ([пробел], +, –, =, &&, ||, >, <, !, (,), {, }, [,], ^, ", ~, *, ?, :, \, /), такие символы в теле запроса необходимо экранировать. Ниже приведены исключения для использования специальных символов в поисковых запросах.

  Для экранирования в Kaspersky CyberTrace используется символ обратной косой черты `\`.

- Использование пробела. Слово, следующее за неэкранированным символом пробела, не будет отнесено к подстроке поиска.

  Пример 1: `supplier_vendor_name: Vendor\ Test` – возвращаются все индикаторы, принадлежащие к источникам с именем поставщика «Vendor Test».

  Пример 2: `supplier_vendor_name: Vendor Test` – возвращаются все индикаторы, принадлежащие к источникам с именем поставщика «Vendor», и индикаторы, у которых в контексте есть слово «test».

- Определенные подстроки могут заключаться в кавычки, а логические блоки могут заключаться в круглые скобки. Для начальных или конечных значений используются фигурные скобки (`{}`) для задания интервалов, исключающих граничные значения, и квадратные скобки (`[]`) для задания интервалов, включающих граничные значения. Фигурные и квадратные скобки можно комбинировать, т.е. задавать интервалы с открывающей скобкой одного вида и закрывающей скобкой другого вида. Кавычки и скобки всех типов в поисковом запросе должны образовывать пары.

  > Не разрешается заключать подстроку поиска в кавычки, если подстрока не содержит специальных символов, перечисленных выше. В этом случае в результаты поиска будут включены только индикаторы, в которых указанная подстрока полностью совпадает с одним из значений любого поля. Поэтому если требуется найти индикаторы, в которых подстрока поиска является лишь частью значения поля, следует использовать подстановочные знаки (звездочка «*» или вопросительный знак «?» — см. ниже).

  Использовать непарные кавычки и все виды непарных скобок можно в следующих случаях:

  - Если непарная скобка или кавычка используется с экранирующим символом.

    Пример: `ioc_value:asd\]`

- Если непарная скобка заключена в кавычки.

  Пример: `ioc_value:"1234]"`

- Запрещается использовать символ табуляции.

- Двоеточие (`:`) следует указывать только после имени атрибута индикатора, в противном случае его необходимо экранировать.

- Не указывайте пустое значение в круглых скобках, за исключением случаев, когда это значение указывается с экранирующим символом или заключается в кавычки.

  Пример неправильного запроса: `( )`

  Пример правильного запроса: `(" ")`

- В фигурных скобках (`{}`) и квадратных скобках (`[]`) следует использовать шаблон `%begin_value% TO %end_value%`, где `%begin_value%` и `%end_value%` — это значения, предназначенные для открытых и закрытых интервалов (кроме случаев, когда квадратные скобки заключены в кавычки).

  Пример неправильного запроса: `[* 100]`

  Пример правильного запроса: `[* TO 100]`

- Не указывайте пустое значение при поиске конкретного атрибута.

  Пример неправильного запроса: `ioc_type:`

  Пример правильного запроса: `ioc_type:url`

- Используйте логические операторы (`AND`, `OR`, `NOT`) без кавычек и только в верхнем регистре.

- Логические `AND`, `OR` должны быть окружены пробелами. Не допускается пробел слева от логического `NOT`, если `NOT` непосредственно следует за левой скобкой или двоеточием.

  Пример неправильного запроса: `supplier_confidence:(89OR91)`

  Пример правильного запроса: `supplier_confidence:NOT(89 OR 91)`

- Не допускается указание пустого значения после логического оператора.

  Пример неправильного запроса: `supplier_confidence:(89 OR )`

  Пример правильного запроса: `supplier_confidence:(89 OR 91)`

- Для атрибута `ioc_supplier_context` следует использовать точку при поиске определенного вложенного атрибута.

  Пример: `ioc_supplier_context.files.threat:"HEUR:Exploit.SWF.Generic"`

- Для атрибута `ioc_supplier_context`, если строка поиска содержит пробелы, следует экранировать пробелы символом "\" (обратная косая черта).

  Пример: `ioc_supplier_context.details.SMS\ Number:1003`

- Для атрибута `ioc_supplier_context` при поиске всех вложенных атрибутов следует использовать запись вида `ioc_supplier_context.\\*`.

  Пример: `ioc_supplier_context.\\*:HEUR`

- В качестве подстановочных знаков в заменителях для любой другой последовательности символов следует использовать звездочку (`*`), а для одиночного символа — вопросительный знак (`?`).

  Пример 1: `supplier_vendor_name: Vendor` – поиск индикаторов, принадлежащих к источникам с именем поставщика «Vendor».

Пример 2: `supplier_vendor_name: Vendor*` – поиск индикаторов, принадлежащих к источникам с именем поставщика, которое начинается с «Vendor».

> Использование звездочки (*) в начале запроса может привести к проверке всех значений атрибутов в базе данных индикатора. Обычно это вызывает долгое ожидание ответа от базы данных.

Примеры

Следующий запрос отображает все индикаторы, содержащие подстроку `at, ca, kr, ru, ir` в любом из атрибутов индикатора:

```
"at, ca, kr, ru, ir"
```

Следующий запрос отображает все индикаторы, у которых значение атрибута `supplier_confidence` равно 89 или 91:

```
supplier_confidence:(89 OR 91)
```

Следующий запрос отображает все индикаторы, у которых значение атрибута `ioc_value` содержит подстроку `123321`:

```
ioc_value:"123321"
```

Следующий запрос отображает все индикаторы, которые были добавлены в базу данных в период с 2012-01-01 по 2012-12-31 (включительно):

```
ioc_created_date:[2012-01-01 TO 2012-12-31]
```

Следующий запрос отображает все индикаторы с уровнем доверия от 10 до 50 (не включительно):

```
supplier_confidence:{10 TO 50}
```

Следующий запрос отображает все индикаторы, у которых значение поля контекста `threat_score` больше `75`:

```
ioc_supplier_context.threat_score:[75 TO *]
```

Следующий запрос отображает все индикаторы, у которых есть атрибут files.threat, содержащий подстроку `HEUR:Exploit.SWF.Generic`:

```
ioc_supplier_context.files.threat:"HEUR:Exploit.SWF.Generic"
```

Следующий запрос отображает все индикаторы, у которых есть атрибуты контекста со значением HEUR на любом уровне вложенности:

```
ioc_supplier_context.\\*:HEUR
```

Управление поисковыми запросами

Веб-интерфейс Kaspersky CyberTrace позволяет работать с поисковыми запросами на странице **Индикаторы**, в том числе выполнять следующие действия:

- Сохранение поисковых запросов
- Просмотр сохраненных поисковых запросов
- Удаление сохраненных поисковых запросов

Для работы с этой страницей необходимо перейти в режим **Управление данными**.

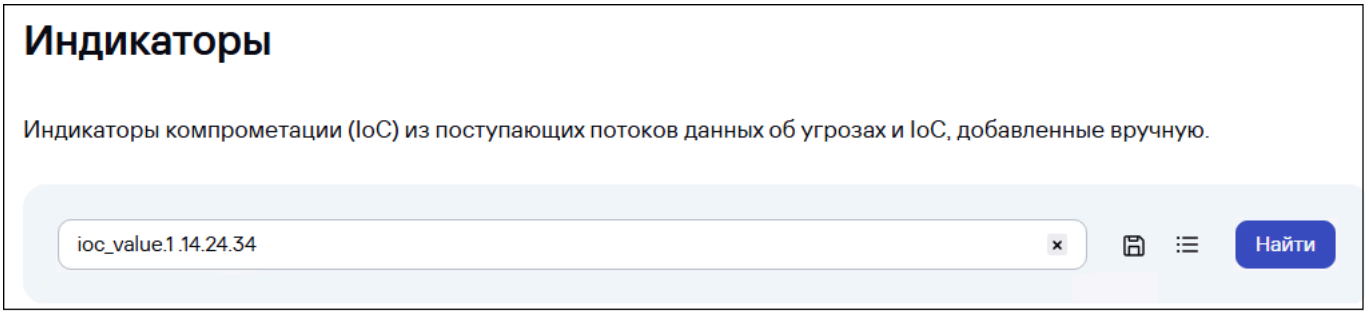
Сохранение поисковых запросов

Для сохранения поискового запроса выполните следующие действия:

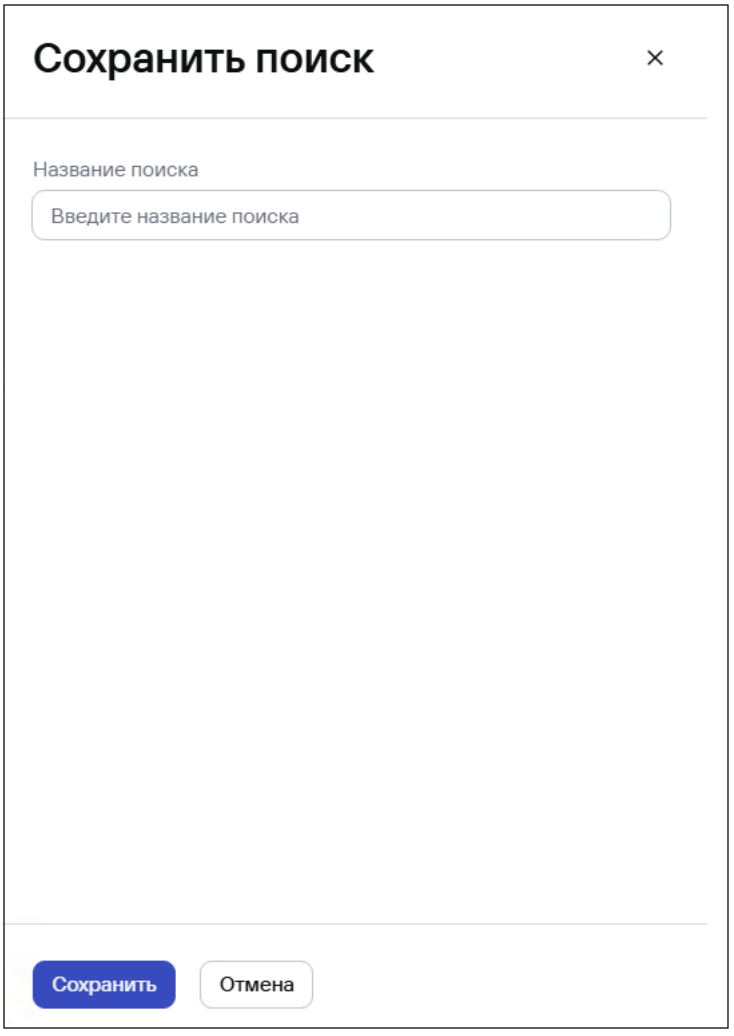
1. На странице **Индикаторы** выполните поиск индикаторов.
2. Нажмите на кнопку (**Сохранить этот поиск**) рядом с полем поиска.
3. В открывшемся окне **Сохранить поиск** введите имя для сохраняемого поискового запроса.

Поисковый запрос сохраняется.

Один пользователь может сохранить не более 1000 поисковых запросов.



Значок **Сохранить этот поиск**



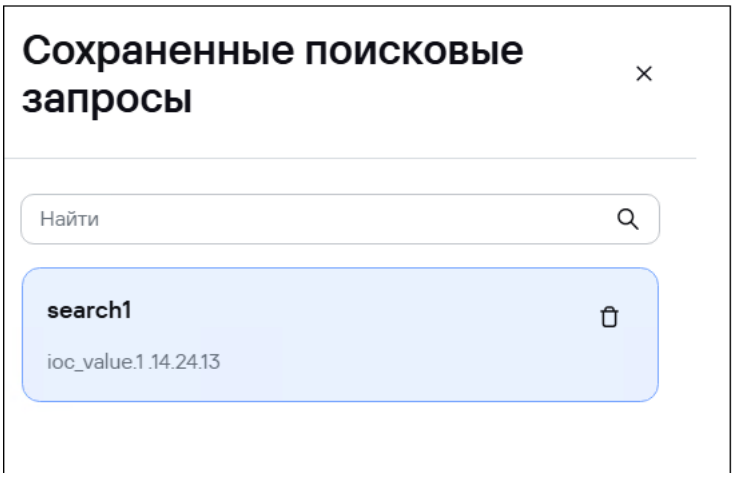
Присвоение имени поисковому запросу

Управление сохраненными поисковыми запросами

Чтобы просмотреть сохраненные поисковые запросы, выполните следующие действия:

На странице **Индикаторы** нажмите на значок ⁝≡ (**Сохраненные поисковые запросы**) рядом с полем поиска.

Откроется окно **Сохраненные поисковые запросы**, в котором отображаются все сохраненные поисковые запросы.



Просмотр сохраненных поисковых запросов

В окне **Сохраненные поисковые запросы** можно выполнять поиск сохраненных поисковых запросов с помощью поля поиска, а также удалять сохраненные поисковые запросы.

Просмотр подробной информации об индикаторах

Для получения подробной информации об индикаторах можно нажать на интересующий индикатор в таблице. Выполняется переход на страницу со следующей информацией:

- Тип запрашиваемого индикатора

  Индикатор может относиться к нескольким типам (например, IP и URL).

- Значение запрашиваемого показателя
- Дата и время, когда был добавлен запрашиваемый индикатор
- Дата и время, когда запрошенный индикатор был обнаружен в первый раз и в последний раз
- Дата и время последнего обновления индикатора
- Отметка, указывающая, принадлежит ли запрошенный индикатор к источнику данных об угрозах *FalsePositive*
- Список источников событий, связанных с запрошенным индикатором
- Список тегов, назначенных индикатору.

На этой странице можно выполнить следующие действия:

- Отметить индикатор как ложное срабатывание или удалить индикатор из списка ложных срабатываний

  Индикатор может принадлежать к нескольким типам. В этом случае выдается запрос о том, индикатор какого типа требуется отметить как ложное срабатывание или удалить из списка ложных срабатываний.

- Удалить индикатор.

  > Удаление индикаторов доступно только пользователям с ролью «Администратор».

- Просмотреть индикатор на графе.
- Просмотреть обнаружения киберугрозы, относящиеся к индикатору.
- Просмотреть информацию об индикаторе на Kaspersky Threat Intelligence Portal.
- Установить или снять флаг, указывающий, следует ли генерировать оповещения об обнаружении индикаторов компрометации после завершения процесса сопоставления.
- Добавить индикатор к источнику данных об угрозах *InternalTI*, в том числе добавить или изменить контекстную информацию и сводку.

  Индикатор может принадлежать к нескольким типам. В этом случае каждый тип индикатора можно добавить в список пользовательских сведений о киберугрозах по отдельности.

- Удалить индикатор из источника данных об угрозах *InternalTI*.

  Индикатор может принадлежать к нескольким типам. В этом случае каждый тип индикатора можно удалить из списка пользовательских сведений о киберугрозах по отдельности.

- Назначить или удалить теги.
- Добавить или удалить комментарии к индикатору.

Обогащение индикаторов из внешних источников

Веб-интерфейс Kaspersky CyberTrace позволяет обогащать индикаторы из Kaspersky Threat Intelligence Portal (далее также Kaspersky TIP) с помощью функций Kaspersky Threat Lookup из Kaspersky TIP API, которые возвращают контекст индикатора.

Обогащение позволяет получить расширенный контекст индикатора в случае, если данных самого индикатора недостаточно.

Для обогащения индикатора требуется добавить внешний источник в разделе **Внешние источники** веб-интерфейса Kaspersky CyberTrace.

> Раздел **Внешние источники** доступен только по лицензии Enterprise TIP.

Управление доступом к Kaspersky Threat Intelligence Portal (Kaspersky TIP)

Перед обогащением индикаторов необходимо настроить доступ к Kaspersky Threat Intelligence Portal (Kaspersky TIP) в режиме **Управление системой**.

В разделе **Настройка → Внешние источники** веб-интерфейса Kaspersky CyberTrace можно выполнить следующие действия:

- Создать доступ к Kaspersky TIP.
- Просмотреть все созданные доступы к Kaspersky TIP.
- Изменить доступ к Kaspersky TIP.
- Удалить доступ к Kaspersky TIP.

Создание доступа к Kaspersky TIP

Чтобы создать доступ к Kaspersky TIP, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите в режим **Управление системой**.
2. Перейдите в раздел **Настройки → Внешние источники**.
3. В открывшемся окне **Внешние источники** нажмите **Добавить внешний источник**.
4. На открывшейся боковой панели **Добавление внешнего источника** укажите следующую информацию:
   - В поле **Имя** задайте имя доступа.

     Имя доступа должно быть уникальным и может содержать только следующие символы:
     - Буквы латинского алфавита (A–Z, a–z)
     - буквы кириллицы (А–Я, а–я)
     - Цифры (0–9)
     - Точка, символ подчеркивания, дефис
   - В поле **Токен доступа** укажите токен API.

     Значение токена API должно содержать от 1 до 2048 символов; допускаются только символы UTF-8.
   - В раскрывающемся списке **Тенанты** выберите один или несколько тенантов, которым вы хотите дать доступ к Kaspersky TIP.

     Для каждого тенанта можно создать только один доступ к Kaspersky TIP. В раскрывающемся списке отображаются только тенанты, у которых нет доступа к Kaspersky TIP.
5. Нажмите на кнопку **Add**.

Доступ к Kaspersky TIP будет создан и появится в окне **Внешние источники**.

Просмотр созданных доступов к Kaspersky TIP

В разделе **Настройка → Внешние источники** можно просмотреть все созданные доступы к Kaspersky TIP.

Для каждого доступа отображается таблица со следующими данными:

- Имя внешнего источника, для которого настроен доступ
- Имя доступа
- Тенанты, имеющие доступ к внешнему источнику

- Суточная квота (количество индикаторов, которые можно обогатить за сутки в рамках тенанта)
- Дата и время истечения срока действия токена API

Изменение доступа к Kaspersky TIP

Чтобы изменить доступ к Kaspersky TIP, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите в режим **Управление системой**.
2. Перейдите в раздел **Настройки** → **Внешние источники**.
3. В открывшемся окне **Внешние источники** нажмите на кнопку **Изменить** ( ) в столбце таблицы **Действия**.
4. На открывшейся боковой панели **Изменение внешнего источника** укажите следующую информацию:
   - В поле **Имя** задайте имя доступа.

     Имя доступа должно быть уникальным и может содержать только следующие символы:
     - Буквы латинского алфавита (A–Z, a–z)
     - буквы кириллицы (А–Я, а–я)
     - Цифры (0–9)
     - Точка, символ подчеркивания, дефис
   - В поле **Токен доступа** укажите токен API.

     Значение токена API должно содержать от 1 до 2048 символов; допускаются только символы UTF-8.
   - В раскрывающемся списке **Тенанты** выберите один или несколько тенантов, для которых будет доступен Kaspersky TIP.
5. Нажмите на кнопку **Save**.

Изменения настроек доступа к Kaspersky TIP будут сохранены. Эти настройки будут автоматически применены для выбранных тенантов.

Удаление доступа к Kaspersky TIP

Чтобы удалить доступ к Kaspersky TIP, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите в режим **Управление системой**.
2. Перейдите в раздел **Настройка** → **Внешние источники**.
3. В открывшемся окне **Внешние источники** нажмите на кнопку **Удалить** ( ) для доступа, который требуется удалить, в столбце таблицы **Действия**.
4. В открывшемся окне подтвердите удаление доступа.

Доступ будет удален.

Просмотр обогащения индикаторов

Вы можете просмотреть обогащение индикатора в разделе **Обогащение из Kaspersky Threat Intelligence Portal** в окне **Сведения об индикаторах**.

В разделе **Обогащение из Kaspersky Threat Intelligence Portal** будет отображаться следующая информация:

- Доступная суточная квота (количество индикаторов, которые можно обогатить за сутки)
- Количество запросов на обогащение, выполненных за последние 24 часа
- Дата и время последнего обновления информации по квоте и запросам

В разделе **Обогащение из Kaspersky Threat Intelligence Portal** вы можете обогатить индикатор, нажав на кнопку **Обогатить**.

Обогащение индикаторов возможно только при наличии действующей лицензии Enterprise TIP и при настроенном доступе к Kaspersky Threat Intelligence Portal.

Обогащение индикатора из Kaspersky Threat Intelligence Portal

Обогащение индикаторов возможно только при наличии действующей лицензии Enterprise TIP, при настроенном доступе к Kaspersky Threat Intelligence Portal и включенном потоке данных Kaspersky Threat Lookup.

Чтобы обогатить индикатор из Kaspersky TIP, выполните действия в следующем порядке:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите в режим **Управление данными**.
2. Перейдите в раздел **Индикаторы**.
3. Выберите индикатор, который вы хотите обогатить, в таблице индикаторов.
4. В открывшемся окне «**Сведения об индикаторах**» в разделе **Обогащение из Kaspersky Threat Intelligence Portal** нажмите кнопку **Обогатить**.

Данные обогащения индикатора появятся в разделе **Обогащение из Kaspersky Threat Intelligence Portal**.

Для просмотра подробной информации об обогащении индикатора можно нажать на кнопку **Показать дополнительную информацию**. Кроме того, данные обогащения можно обновить нажатием на кнопку **Обновить данные**.

Управление потоком данных Kaspersky Threat Lookup

Индикаторы, предоставляющие контекст от сторонних служб, записываются в отдельные потоки данных.

При обогащении индикаторов из Kaspersky Threat Intelligence Portal создается поток данных Kaspersky Threat Lookup. В этом потоке данных хранятся все индикаторы и их контекст, полученные с помощью Kaspersky Threat Intelligence Portal.

Если у тенанта есть поток данных Kaspersky Threat Lookup, он отображается в разделе **Потоки данных** в режиме **Управление данными**.

Администраторы и менеджеры тенантов могут просматривать, включать, выключать и настраивать этот поток данных.

Просмотр потока данных Kaspersky Threat Lookup

Чтобы просмотреть поток данных Kaspersky Threat Lookup, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите в режим **Управление данными**.
2. Перейдите в раздел **Настройка** → **Потоки данных**.
3. В открывшемся окне **Потоки данных** перейдите на вкладку **Обогащение**.

   Поток данных отображается в виде таблицы со следующими столбцами: **Состояние**, **Название**, **Описание**, **Действия**.

Поток данных Kaspersky Threat Lookup также отображается в разделах **Ретроскан** и **Обнаружения**.

Включение и выключение потока данных Kaspersky Threat Lookup

По умолчанию поток данных Kaspersky Threat Lookup включен.

Чтобы включить или выключить поток данных:

1. Перейдите в раздел **Настройки** → **Потоки данных**.
2. Перейдите на вкладку **Обогащение**.
3. Включите или выключите переключатель потока данных Kaspersky Threat Lookup в столбце **Состояние**.

Настройка потока данных Kaspersky Threat Lookup

Чтобы настроить поток данных Kaspersky Threat Lookup, выполните следующие действия:

1. Перейдите в раздел **Настройки** → **Потоки данных**.
2. Перейдите на вкладку **Обогащение**.
3. В столбце **Действия** нажмите на кнопку настройки ( ).
4. В открывшейся боковой панели потока данных Kaspersky Threat Lookup выполните следующие действия:

   - Включите или выключите поток данных.
   - Выберите доступные поля для потока данных об угрозах.

     Для успешного применения параметров необходимо выбрать все следующие поля: **MD5**, **SHA1**, **SHA256**, **IP**, **URL**.

- Просмотрите уровень доверия к потоку данных.
- Добавьте поля контекста для потока данных.

5. Нажмите на кнопку **Сохранить**.

Поток данных Kaspersky Threat Lookup будет настроен.

Информация о доступных полях, уровне доверия и полях контекста приведена в статье Настройка потоков данных.

Скачивание отчетов из Kaspersky Threat Intelligence Portal

Вы можете скачать отчеты и связанные с ними артефакты (IOC, YARA-правила и правила для решений IDS/IPS) для индикаторов потоков данных APT или Crimeware из Kaspersky Threat Intelligence Portal. Перед скачиванием отчета убедитесь, что у вас имеется лицензия TIP Enterprise и доступ к Kaspersky Threat Intelligence Portal. Также вам понадобится API-токен с лицензией Kaspersky Intelligence Reporting.

Чтобы скачать отчет для индикатора из Kaspersky Threat Intelligence Portal:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите в режим **Управление данными**.
2. Перейдите в раздел **Индикаторы**.
3. Выберите индикатор, который вы хотите просмотреть, в таблице индикаторов.
4. В окне **Сведения об индикаторе** нажмите на кнопку **Скачать отчет**.

   Скачивание отчета возможно только в том случае, если поток данных типа APT или Crimeware, а в потоке данных индикатора имеется поле api_publication_id.
5. В раскрывающемся списке выберите один из следующих параметров отчета:
   - **Все доступные** – все файлы публикации, доступные для индикатора
   - **PDF** – полный отчет в формате PDF
   - **Сводка** – краткий отчет в формате PDF
   - **YARA** – отчет в формате YARA-правил
   - **IOC** – файл с IOC
   - **Suricata** – файл с правилами для решений IDS/IPS для соответствующего отчета

Отчет для индикатора будет скачан.

Экспорт индикаторов в CSV

Вы можете экспортировать индикаторы в файл CSV на странице **"Индикаторы"**.

Файл CSV будет содержать индикаторы, которые будут отображаться в таблице индикаторов на момент экспорта.

Вы можете настроить отображаемые индикаторы с помощью поиска индикаторов по атрибутам, а также фильтрации и сортировки столбцов таблицы индикаторов.

Чтобы экспортировать индикаторы:

1. Перейдите в режим "Управление данными".
2. Перейдите на страницу **"Индикаторы"**.
3. Нажмите на иконку (экспорт) над таблицей индикаторов.

Индикаторы будут экспортированы в файл CSV.

Файл CSV соответствует следующим требованиям:

- Первая строка файла начинается с символа хеша (#), за которым следуют заголовки.
- Заголовки разделяются точкой с запятой (;).
- Значения разделяются точкой с запятой (;).
- Набор столбцов и их порядок соответствуют параметрам запроса.
- В файле будет указано не более 1000 индикаторов.
- Имена заголовков в первой строке соответствуют именам столбцов таблицы индикаторов в веб-интерфейсе.
- Имя файла имеет следующий формат: `Indicators_%date%.csv`, где `%date%` – дата создания файла в формате ГГГГ-ММ-ДД.

Работа со списком пользовательских сведений о киберугрозах

На странице **Индикаторы** можно работать со списком индикаторов, добавленных в список пользовательских сведений о киберугрозах. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Чтобы приступить к работе со списком пользовательских сведений о киберугрозах, необходимо выполнить следующие действия:

1. Нажмите на кнопку **Управлять пользовательским списком индикаторов**.
2. Выберите тип индикатора.

3. Если требуется, внесите изменения в список значений. Каждое значение должно начинаться с новой строки.

   Kaspersky CyberTrace применяет правила нормализации URL ко всем добавляемым URL, которые еще не содержатся в базе данных индикаторов. Таким образом, представление того или иного URL может изменяться. Например, при добавлении URL, содержащего порт, значение порта удаляется.

4. Нажмите на кнопку **Сохранить**.

Список индикаторов с *InternalTI* в значении атрибута `suppliers_name` будет обновлен.

Экспорт индикаторов в NGFW

Сетевые экраны нового поколения (NGFW) предоставляют возможность фильтрации DNS- и веб-трафика с использованием внешних динамических списков индикаторов компрометации.

Вы можете создать задачу для экспорта индикаторов в выбранный NGFW. В этой задаче можно настроить экспорт индикаторов в зависимости от выбранного NGFW. Предварительно заданные вами параметры будут сохранены и могут быть изменены при необходимости.

Чтобы создать задачу экспорта индикаторов для NGFW:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите в режим **Управление системой**.
2. Перейдите в раздел **Настройки** → **Экспорт индикаторов**.
3. В открывшемся окне **Экспорт индикаторов** нажмите на кнопку **Добавить задачу** и выберите требуемый NGFW в раскрывающемся списке.
4. В открывшемся окне **Добавить задачу экспорта индикаторов** задайте следующие параметры:
   - В поле **Имя задачи** укажите уникальное имя задачи.
   - В поле **Экспортировать каждые** укажите частоту запуска задачи.
   - В поле **Максимальное количество записей** укажите количество экспортируемых индикаторов в зависимости от выбранного NGFW.

     Максимальное значение, которое можно указать – 1 000 000.
   - В поле **Тип файла** укажите тип файла.
   - В поле **Тип индикатора** укажите тип индикатора.

     Вы можете указать один или несколько типов индикаторов для выбранного NGFW в соответствии с таблицей **"Параметры экспорта для NGFW"** ниже.
5. В разделах **Правила фильтрации** и **Условия сортировки** настройте фильтрацию и сортировку индикаторов.
6. Настройте ограничения доступа к файлу экспорта индикаторов.

   Для этого включите переключатель **Использовать авторизацию для загрузки отчета об экспорте индикаторов** и укажите имя пользователя и пароль.

7. Нажмите на кнопку **Next**.

8. В открывшемся окне **Предварительный просмотр экспорта** просмотрите файл экспорта.

9. Нажмите на кнопку **Add**.

Задача будет создана. Также в окне **Экспорт индикаторов** отображается ссылка на скачивание файла с экспортированными индикаторами и столбец с типом задачи экспорта. Если для задачи имеются предустановленные параметры, в столбце будет указано название NGFW. Если у задачи нет предустановленных параметров, в столбце будет указано значение `"Универсальный экспорт в CSV"`.

Задача экспорта NGFW будет отображаться в разделе **Задачи** в режиме **Управление системой**.

После создания задачи вам потребуется добавить экспортированные индикаторы в NGFW. Для этого перейдите по ссылкам для каждого NGFW в таблице ниже. Эта таблица содержит параметры, которые можно использовать для экспорта индикаторов в различные NGFW:

Параметры экспорта для NGFW

Имя NGFW	Рекомендуемое количество индикаторов для одного экспорта (по умолчанию)	Доступные типы IoC	Тип файла
Check Point NGFW	500 000	Одно или более из следующих: • IP • Домен	.CSV
Cisco Firewall Management Center	100 000	Одно из следующих: • IP • URL • Домен • SHA256	.CSV
FortiGate	131 000	Одно из следующих: • IP • URL • Домен • HASH • MD5 • SHA1 • SHA256	.TXT .CSV Без типа
Palo Alto NGFW	50 000	Одно из следующих: • IP • URL • Домен	.CSV
Sophos Firewall	50 000	Одно из следующих: • IP • URL • Домен	.TXT .CSV Без типа
Security Code Continent NGFW	50 000	Одно или более из следующих: • IP • URL • Домен • MD5	.JSON
UserGate	50 000	Одно из следующих: • IP • URL • Домен	Два файла: • version.txt (версия с потоками данных) • list.zip с файлом list.txt (архив с индикаторами)

Broadcom (Symantec) ProxySG	50 000	Одно из следующих: • IP • Домен	.TXT .CSV Без типа

Экспорт индикаторов в Check Point NGFW

В этом разделе описано, как интегрировать Kaspersky CyberTrace с Check Point NGFW, создать задачу экспорта индикаторов из Kaspersky CyberTrace и добавить индикаторы в Check Point NGFW.

Check Point NGFW поддерживает работу со сторонними потоками данных IoC. Эти потоки данных можно добавить как объекты сетевого потока данных (содержащие IP-адреса или URL) и использовать в качестве исходного или целевого объекта в базе правил. Кроме того, эти потоки данных можно добавить с помощью функции пользовательских потоков данных об угрозах.

Создание задачи экспорта индикаторов из Kaspersky CyberTrace

В разделе **Экспорт индикаторов** можно создать или обновить задачи для предустановленных параметров экспорта индикаторов в Check Point NGFW.

Чтобы создать задачу экспорта индикаторов из Kaspersky CyberTrace, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите в режим **Управление системой**.
2. Перейдите в раздел **Настройки** → **Экспорт индикаторов**.
3. В открывшемся окне **Экспорт индикаторов** нажмите на кнопку **Добавить задачу** и выберите **Check Point NGFW** в раскрывающемся списке.
4. В открывшемся окне **Добавить задачу экспорта индикаторов** задайте следующие параметры:
   - В поле **Имя задачи** укажите уникальное имя задачи.
   - В поле **Экспортировать каждые** укажите частоту запуска задачи.
   - В поле **Максимальное количество записей** укажите количество экспортируемых индикаторов.

     Рекомендуемое количество индикаторов для одного экспорта (по умолчанию) составляет 500 000.

     Максимальное значение: 1 000 000.
   - В поле **Тип файла** укажите тип файла.

     Тип файла Check Point NGFW – `.CSV`.
   - В поле **Тип индикатора** укажите тип индикатора.

     Доступные типы индикаторов: **IP-адрес**, **домен**.
5. В разделах **Правила фильтрации** и **Условия сортировки** настройте фильтрацию и сортировку индикаторов.

   Подробнее о фильтрации и сортировке индикаторов см. в статье Параметры экспорта индикаторов.
6. Настройте ограничения доступа к файлу экспорта индикаторов.

   Для этого включите переключатель **Использовать авторизацию для загрузки отчета об экспорте индикаторов** и укажите имя пользователя и пароль.

7. Нажмите на кнопку **Next**.

8. В открывшемся окне **Предварительный просмотр экспорта** просмотрите файл экспорта.

9. Нажмите на кнопку **Add**.

Задача будет создана.

В окне **экспорта индикаторов** будет отображаться столбец с типом задачи экспорта. Если для задачи имеются предустановленные параметры, в столбце будет указано имя NGFW.

Предварительно установленная задача экспорта будет отображена в разделе **Задачи** в режиме **Управление системой**.

В разделе **"Экспорт индикаторов"** отображается ссылка на скачивание файла для предварительно установленной задачи экспорта.

Добавление индикаторов в Check Point NGFW

После экспорта индикаторов из Kaspersky CyberTrace файл с экспортированными индикаторами становится доступным для скачивания по следующему адресу:

```
https://<CyberTrace_WebAddress>/ioc_exports/<iocexport_name>
```

где `<iocexport_name>` – имя вашей задачи экспорта.

Чтобы добавить индикаторы в Check Point NGFW,

укажите приведенный выше URL файла с экспортированными индикаторами в окне **Новый сетевой поток данных** интерфейса Check Point NGFW.

Указывать имя пользователя и пароль (api_token) может не требоваться, если задача экспорта IoC из Kaspersky CyberTrace создана без базовой аутентификации.

Подробную информацию о добавлении индикаторов см. в аналогичном руководстве по добавлению потоков данных Kaspersky Network Security в Check Point NGFW.

Экспорт индикаторов в FortiGate NGFW

В этой статье описывается порядок интеграции Kaspersky CyberTrace с FortiGate NGFW, создания задачи экспорта индикаторов из Kaspersky CyberTrace и добавления индикаторов в FortiGate NGFW.

FortiGate NGFW основан на операционной системе FortiOS®. Начиная с версии 6.0, FortiOS поддерживает внешние динамические списки IoC в виде обновляемых текстовых файлов, расположенных на веб-сервере и доступных по HTTP/HTTPS.

После импорта IoC в FortiGate их можно использовать в различных политиках в зависимости от типа IoC (веб-фильтр, DNS-фильтр, профиль антивируса), а также в качестве источника/назначения в политиках IPv4 и прокси.

Для интеграции требуется коммерческая лицензия FortiGate.

Создание задачи экспорта индикаторов из Kaspersky CyberTrace

В разделе **"Экспорт индикаторов"** вы можете создать или обновить задачу для предварительно заданных параметров экспорта индикаторов в FortiGate NGFW.

Чтобы создать задачу экспорта индикаторов из Kaspersky CyberTrace, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите в режим **Управление системой**.
2. Перейдите в раздел **Настройки** → **Экспорт индикаторов**.
3. В открывшемся окне **Экспорт индикаторов** нажмите на кнопку **Добавить задачу**, а затем выберите **FortiGate NGFW** из раскрывающегося списка.
4. В окне **Добавить задачу экспорта индикаторов** укажите следующие свойства:
   - В поле **Имя задачи** укажите уникальное имя задачи.
   - В поле **Экспортировать каждые** укажите частоту запуска задачи.
   - В поле **Максимальное количество записей** укажите количество экспортируемых индикаторов.

     Рекомендуемое количество индикаторов для одного экспорта (по умолчанию) составляет 131 000.

     Максимальное значение: 1 000 000.
   - В поле **Тип файла** укажите тип файла.

     Для FortiGate NGFW это `.txt`, `.csv` и файлы без типа.
   - Тип индикатора в поле **"Тип IoC"**.

     Доступные типы индикаторов: **IP**, **URL**, **Domain**, **Hash**, **MD5**, **SHA1**, **SHA256**.
5. В разделах **Правила фильтрации** и **Условия сортировки** настройте фильтрацию и сортировку индикаторов.
6. Настройте ограничения доступа к файлу экспорта индикаторов.

   Для этого включите переключатель **Использовать авторизацию для загрузки отчета об экспорте индикаторов** и укажите имя пользователя и пароль.
7. Нажмите на кнопку **Next**.
8. В открывшемся окне **Предварительный просмотр экспорта** просмотрите файл экспорта.
9. Нажмите на кнопку **Add**.

Задача будет создана.

В окне **экспорта индикаторов** будет отображаться столбец с типом задачи экспорта. Если для задачи имеются предустановленные параметры, в столбце будет указано имя NGFW.

Предварительно установленная задача экспорта будет отображена в разделе **Задачи** в режиме **Управление системой**.

В окне **экспорта индикаторов** отображается ссылка на скачивание файла для предварительно установленной задачи экспорта.

Добавление индикаторов в FortiGate NGFW

После экспорта индикаторов из Kaspersky CyberTrace файл с экспортированными индикаторами становится доступным для скачивания по следующему адресу:

```
https://<CyberTrace_WebAddress>/ioc_exports/<iocexport_name>
```

где `<iocexport_name>` – имя вашей задачи экспорта.

Чтобы добавить индикаторы в FortiGate NGFW,

укажите URL файла с экспортированными индикаторами в поле **URL внешнего ресурса** окна **Новый внешний коннектор** интерфейса FortiGate NGFW.

Указывать имя пользователя и пароль (api_token) может не требоваться, если задача экспорта IoC из Kaspersky CyberTrace создана без базовой аутентификации.

Подробную информацию о добавлении индикаторов см. в аналогичном руководстве по добавлению потоков данных Kaspersky Network Security в FortiGate NGFW.

Экспорт индикаторов в UserGate NGFW

В этой статье описывается порядок интеграции Kaspersky CyberTrace с UserGate NGFW, создания задачи экспорта индикаторов из Kaspersky CyberTrace и добавления индикаторов в UserGate NGFW.

Kaspersky CyberTrace позволяет экспортировать списки индикаторов компрометации (IoC) в сетевые экраны нового поколения (NGFW) UserGate, расширяя возможности по обнаружению и предотвращению киберугроз.

Создание задачи экспорта индикаторов из Kaspersky CyberTrace

В разделе **"Экспорт индикаторов"** вы можете создать или обновить задачу для предварительно заданных параметров экспорта индикаторов в UserGate NGFW.

Чтобы создать задачу экспорта индикаторов из Kaspersky CyberTrace, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите в режим **Управление системой**.
2. Перейдите в раздел **Настройки** → **Экспорт индикаторов**.
3. В открывшемся окне **Экспорт индикаторов** нажмите на кнопку **Добавить задачу** и выберите **UserGate NGFW** в раскрывающемся списке.
4. В окне **Добавить задачу экспорта индикаторов** укажите следующие свойства:
   - В поле **Имя задачи** укажите уникальное имя задачи.
   - В поле **Экспортировать каждые** укажите частоту запуска задачи.
   - В поле **Максимальное количество записей** укажите количество экспортируемых индикаторов.

     Рекомендуемое количество индикаторов для одного экспорта (по умолчанию) составляет 50 000.

     Максимальное значение, которое можно указать – 1 000 000.

- В поле **Тип файла** укажите тип файла.

  Для UserGate NGFW это `version.txt` (версия потоков данных) и `list.zip` с `list.txt` (архив с индикаторами).

- В поле **Тип индикатора** укажите тип индикатора.

  Доступные типы индикаторов: **IP-адрес**, **URL**, **домен**.

5. В разделах **Правила фильтрации** и **Условия сортировки** настройте фильтрацию и сортировку индикаторов.

6. Настройте ограничения доступа к файлу экспорта индикаторов.

   Для этого включите переключатель **Использовать авторизацию для загрузки отчета об экспорте индикаторов** и укажите имя пользователя и пароль.

7. Нажмите на кнопку **Next**.

8. В открывшемся окне **Предварительный просмотр экспорта** просмотрите файл экспорта.

9. Нажмите на кнопку **Add**.

Задача будет создана.

В окне **экспорта индикаторов** будет отображаться столбец с типом задачи экспорта. Если для задачи имеются предустановленные параметры, в столбце будет указано имя NGFW.

Предварительно установленная задача экспорта будет отображена в разделе **Задачи** в режиме **Управление системой**.

В окне **экспорта индикаторов** отображается ссылка на скачивание файла для предварительно установленной задачи экспорта.

В окне **Экспорт индикаторов** отображается неполная ссылка (только для чтения) на каталог с файлами `version.txt` и `list.zip`. Чтобы скачать файл, вам нужно добавить в эту ссылку имена файлов: `version.txt` или `list.zip`. Если вы используете ссылку в UserGate, менять ее не требуется.

Добавление индикаторов в UserGate NGFW

После экспорта индикаторов из Kaspersky CyberTrace файл с экспортированными индикаторами становится доступным для скачивания по следующему адресу:

```
https://<CyberTrace_WebAddress>/ioc_exports/<iocexport_name>
```

где `<iocexport_name>` – имя вашей задачи экспорта.

Чтобы добавить индикаторы в UserGate NGFW,

укажите приведенный выше URL файла с экспортированными индикаторами в окне **Списки URL** интерфейса UserGate NGFW.

Сетевые экраны UserGate не поддерживают аутентификацию при импорте списков IoC из внешних ресурсов и не работают с использованием протокола HTTPS. Интеграция с Kaspersky CyberTrace возможна только через промежуточный обратный прокси.

Подробную информацию о добавлении индикаторов см. в аналогичном руководстве по добавлению потоков данных Kaspersky Network Security в UserGate NGFW.

Экспорт индикаторов в Palo Alto NGFW

В этой статье описывается порядок интеграции Kaspersky CyberTrace с Palo Alto NGFW, создания задачи экспорта индикаторов из Kaspersky CyberTrace и добавления индикаторов в Palo Alto NGFW.

Palo Alto NGFW поддерживает внешние динамические списки IoC в виде обновляемых текстовых файлов, доступных через HTTP/HTTPS.

После импорта в Palo Alto NGFW индикаторы компрометации можно использовать в политиках фильтрации трафика.

Создание задачи экспорта индикаторов из Kaspersky CyberTrace

В разделе **"Экспорт индикаторов"** вы можете создать или обновить задачу для предварительно заданных параметров экспорта индикаторов в Palo Alto NGFW.

Чтобы создать задачу экспорта индикаторов из Kaspersky CyberTrace, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите в режим **Управление системой**.
2. Перейдите в раздел **Настройки** → **Экспорт индикаторов**.
3. В открывшемся окне **Экспорт индикаторов** нажмите на кнопку **Добавить задачу** и выберите **Palo Alto NGFW** в раскрывающемся списке.
4. В окне **Добавить задачу экспорта индикаторов** укажите следующие свойства:
   - В поле **Имя задачи** укажите уникальное имя задачи.
   - В поле **Экспортировать каждые** укажите частоту запуска задачи.
   - В поле **Максимальное количество записей** укажите количество экспортируемых индикаторов.

     Рекомендуемое количество индикаторов для одного экспорта (по умолчанию) составляет 50 000.

     Максимальное значение, которое можно указать – 1 000 000.
   - В поле **Тип файла** укажите тип файла.

     Тип файла Palo Alto NGFW – `.csv`.
   - Тип индикатора в поле **"Тип IoC"**.

     Доступные типы индикаторов: **IP-адрес**, **URL**, **домен**.
5. В разделах **Правила фильтрации** и **Условия сортировки** настройте фильтрацию и сортировку индикаторов.
6. Настройте ограничения доступа к файлу экспорта индикаторов.

   Для этого включите переключатель **Использовать авторизацию для загрузки отчета об экспорте индикаторов** и укажите имя пользователя и пароль.
7. Нажмите на кнопку **Next**.

8. В открывшемся окне **Предварительный просмотр экспорта** просмотрите файл экспорта.

9. Нажмите на кнопку **Add**.

Задача будет создана.

В окне **экспорта индикаторов** будет отображаться столбец с типом задачи экспорта. Если для задачи имеются предустановленные параметры, в столбце будет указано имя NGFW.

Предварительно установленная задача экспорта будет отображена в разделе **Задачи** в режиме **Управление системой**.

В окне **экспорта индикаторов** отображается ссылка на скачивание файла для предварительно установленной задачи экспорта.

Добавление индикаторов в Palo Alto NGFW

После экспорта индикаторов из Kaspersky CyberTrace файл с экспортированными индикаторами становится доступным для скачивания по следующему адресу:

```
https://<CyberTrace_WebAddress>/ioc_exports/<iocexport_name>
```

где `<iocexport_name>` – имя вашей задачи экспорта.

Чтобы добавить индикаторы в Palo Alto NGFW,

укажите приведенный выше URL файла с экспортированными индикаторами в окне **External Dynamic Lists** интерфейса Palo Alto NGFW.

Указывать имя пользователя и пароль (api_token) может не требоваться, если задача экспорта IoC из Kaspersky CyberTrace создана без базовой аутентификации.

Подробную информацию о добавлении индикаторов см. в аналогичном руководстве по добавлению потоков данных Kaspersky Network Security в Palo Alto NGFW.

Экспорт индикаторов в Cisco Firewall Management Center

В этой статье описывается порядок интеграции Kaspersky CyberTrace с Cisco FireWall Management Center, создания задачи экспорта индикаторов из Kaspersky CyberTrace и добавления индикаторов в Cisco FireWall Management Center.

Cisco FireWall Management Center используется для управления сетевыми экранами Cisco (например, Cisco ASA).

Создание задачи экспорта индикаторов из Kaspersky CyberTrace

В разделе **"Экспорт индикаторов"** вы можете создать или обновить задачу для предварительно заданных параметров экспорта индикаторов в Cisco Firewall Management Center.

Чтобы создать задачу экспорта индикаторов из Kaspersky CyberTrace, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите в режим **Управление системой**.
2. Перейдите в раздел **Настройки** → **Экспорт индикаторов**.
3. В открывшемся окне **Экспорт индикаторов** нажмите на кнопку **Добавить задачу** и выберите **Cisco Firewall Management Center** в раскрывающемся списке.
4. В окне **Добавить задачу экспорта индикаторов** укажите следующие свойства:
   - В поле **Имя задачи** укажите уникальное имя задачи.
   - В поле **Экспортировать каждые** укажите частоту запуска задачи.
   - В поле **Максимальное количество записей** укажите количество экспортируемых индикаторов.

     Рекомендуемое количество индикаторов для одного экспорта (по умолчанию) составляет 100 000.

     Максимальное значение, которое можно указать – 1 000 000.
   - В поле **Тип файла** укажите тип файла.

     Тип файла – `.csv`.
   - В поле **Тип индикатора** укажите тип индикатора.

     Доступные типы индикаторов: **IP-адрес**, **URL**, **домен**, **SHA256**.
5. В разделах **Правила фильтрации** и **Условия сортировки** настройте фильтрацию и сортировку индикаторов.
6. Настройте ограничения доступа к файлу экспорта индикаторов.

   Для этого включите переключатель **Использовать авторизацию для загрузки отчета об экспорте индикаторов** и укажите имя пользователя и пароль.
7. Нажмите на кнопку **Next**.
8. В открывшемся окне **Предварительный просмотр экспорта** просмотрите файл экспорта.
9. Нажмите на кнопку **Add**.

Задача будет создана.

В окне **экспорта индикаторов** будет отображаться столбец с типом задачи экспорта. Если для задачи имеются предустановленные параметры, в столбце будет указано имя NGFW.

Предварительно установленная задача экспорта будет отображена в разделе **Задачи** в режиме **Управление системой**.

В разделе **"Экспорт индикаторов"** отображается ссылка на скачивание файла для предварительно установленной задачи экспорта.

Добавление индикаторов в Cisco Firewall Management Center

После экспорта индикаторов из Kaspersky CyberTrace файл с экспортированными индикаторами становится доступным для скачивания по следующему адресу:

`https://<CyberTrace_WebAddress>/ioc_exports/<iocexport_name>`

где `<iocexport_name>` – имя вашей задачи экспорта.

Чтобы добавить индикаторы в Cisco Firewall Management Center:

1. В интерфейсе Cisco Firewall Management Center перейдите в раздел **Интеграция** → **Аналитика** → **Источники**.
2. Нажмите **Добавить новый источник**.
3. В окне **Добавить источник** укажите URL для скачивания файла с экспортированными индикаторами.

Указывать имя пользователя и пароль (api_token) может не требоваться, если задача экспорта IoC из Kaspersky CyberTrace создана без базовой аутентификации.

Подробную информацию о добавлении индикаторов см. в аналогичном руководстве по добавлению потоков данных Kaspersky Network Security в Cisco Firewall Management Center.

Экспорт индикаторов в Sophos Firewall

В этой статье описывается порядок интеграции Kaspersky CyberTrace с Sophos Firewall, создания задачи экспорта индикаторов из Kaspersky CyberTrace и добавления индикаторов в Sophos Firewall.

Sophos Firewall – это полноценный сетевой экран нового поколения, оптимизированный для работы с современным шифрованием в Интернете.

Создание задачи экспорта индикаторов из Kaspersky CyberTrace

В разделе **"Экспорт индикаторов"** вы можете создать или обновить задачу для предварительно заданных параметров экспорта индикаторов в Sophos Firewall.

Чтобы создать задачу экспорта индикаторов из Kaspersky CyberTrace, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите в режим **Управление системой**.
2. Перейдите в раздел **Настройки** → **Экспорт индикаторов**.
3. В открывшемся окне **Экспорт индикаторов** нажмите на кнопку **Добавить задачу** и выберите **Sophos Firewall** в раскрывающемся списке.
4. В окне **Добавить задачу экспорта индикаторов** укажите следующие свойства:
   - В поле **Имя задачи** укажите уникальное имя задачи.
   - В поле **Экспортировать каждые** укажите частоту запуска задачи.
   - В поле **Максимальное количество записей** укажите количество экспортируемых индикаторов. Рекомендуемое количество индикаторов для одного экспорта (по умолчанию) составляет 50 000. Максимальное значение, которое можно указать – 1 000 000.

- В поле **Тип файла** укажите тип файла.

  Для Sophos Firewall тип файла – `.txt`, `.csv`, без типа.

- В поле **Тип индикатора** укажите тип индикатора.

  Доступные типы индикаторов: IP, URL, домен.

5. В разделах **Правила фильтрации** и **Условия сортировки** настройте фильтрацию и сортировку индикаторов.

6. Настройте ограничения доступа к файлу экспорта индикаторов.

   Для этого включите переключатель **Использовать авторизацию для загрузки отчета об экспорте индикаторов** и укажите имя пользователя и пароль.

7. Нажмите на кнопку **Next**.

8. В открывшемся окне **Предварительный просмотр экспорта** просмотрите файл экспорта.

9. Нажмите на кнопку **Add**.

Задача будет создана.

В окне **экспорта индикаторов** будет отображаться столбец с типом задачи экспорта. Если для задачи имеются предустановленные параметры, в столбце будет указано имя NGFW.

Предварительно установленная задача экспорта будет отображена в разделе **Задачи** в режиме **Управление системой**.

В разделе **"Экспорт индикаторов"** отображается ссылка на скачивание файла для предварительно установленной задачи экспорта.

Добавление индикаторов в Sophos Firewall

После экспорта индикаторов из Kaspersky CyberTrace файл с экспортированными индикаторами становится доступным для скачивания по следующему адресу:

```
https://<CyberTrace_WebAddress>/ioc_exports/<iocexport_name>
```

где `<iocexport_name>` – имя вашей задачи экспорта.

Чтобы добавить индикаторы в Sophos Firewall:

1. В интерфейсе брандмауэра Sophos перейдите в **Активное реагирование на угрозы** → **Сторонние потоки данных об угрозах** и нажмите **Добавить**.

2. Укажите URL для скачивания файла с экспортированными индикаторами.

Указывать имя пользователя и пароль (api_token) может не требоваться, если задача экспорта IoC из Kaspersky CyberTrace создана без базовой аутентификации.

Подробную информацию о добавлении индикаторов см. в аналогичном руководстве по добавлению потоков данных Kaspersky Network Security в Sophos Firewall.

Экспорт индикаторов в Broadcom (Symantec) ProxySG

В этой статье описывается порядок интеграции Kaspersky CyberTrace с Broadcom (Symantec™) ProxySG™, создания задачи экспорта индикаторов из Kaspersky CyberTrace и добавления индикаторов в Broadcom (Symantec) ProxySG.

Устройства Broadcom ProxySG хорошо защищены, имеют высокую производительность, просты в использовании и позволяют организациям обеспечивать безопасность и ускорять работу своих веб-приложений и общедоступных сайтов.

Создание задачи экспорта индикаторов из Kaspersky CyberTrace

На странице **"Экспорт индикаторов"** вы можете создать или обновить задачу для предварительно заданных параметров экспорта индикаторов в Broadcom (Symantec) ProxySG.

Чтобы создать задачу экспорта индикаторов из Kaspersky CyberTrace, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите в режим **Управление системой**.
2. Перейдите в раздел **Настройки** → **Экспорт индикаторов**.
3. В открывшемся окне **Экспорт индикаторов** нажмите на кнопку **Добавить задачу** и выберите **Broadcom (Symantec) ProxySG** в раскрывающемся списке.
4. В окне **Добавить задачу экспорта индикаторов** укажите следующие свойства:
   - В поле **Имя задачи** укажите уникальное имя задачи.
   - В поле **Экспортировать каждые** укажите частоту запуска задачи.
   - В поле **Максимальное количество записей** укажите количество экспортируемых индикаторов.
     Рекомендуемое количество индикаторов для одного экспорта (по умолчанию) составляет 50 000.
     Максимальное значение, которое можно указать – 1 000 000.
   - В поле **Тип файла** укажите тип файла.
     Тип файла – `.txt`, `.csv`, без типа.
   - В поле **Тип индикатора** укажите тип индикатора.
     Доступные типы индикаторов: **IP-адрес**, **домен**.
   - В поле **Определите категорию** укажите название категории индикаторов.
     По умолчанию категория индикаторов – `Block_Sites`.
     Название категории может содержать следующие символы:
     - Буквы латинского алфавита (A–Z, a–z)
     - Цифры от 0 до 9
     - Нижнее подчеркивание (_)

5. В разделах **Правила фильтрации** и **Условия сортировки** настройте фильтрацию и сортировку индикаторов.

6. Настройте ограничения доступа к файлу экспорта индикаторов.

   Для этого включите переключатель **Использовать авторизацию для загрузки отчета об экспорте индикаторов** и укажите имя пользователя и пароль.

7. Нажмите на кнопку **Next**.

8. В открывшемся окне **Предварительный просмотр экспорта** просмотрите файл экспорта.

9. Нажмите на кнопку **Add**.

   Задача будет создана. Также в окне **Экспорт индикаторов** отображается ссылка на скачивание файла с экспортированными индикаторами.

В файле экспорта для Broadcom (Symantec) ProxySG для списка значений индикаторов заголовки указаны в первой строке (`define category %category_name%`), а нижний колонтитул – в последней (`end`), как показано в примере ниже:

```
define category Blocked_Sites
80.89.237.223
5.39.127.35
95.216.5.119
80.240.19.33
195.161.41.216
103.71.21.107
end
```

В окне **экспорта индикаторов** будет отображаться столбец с типом задачи экспорта. Если для задачи имеются предустановленные параметры, в столбце будет указано имя NGFW.

Предварительно установленная задача экспорта будет отображена в разделе **Задачи** в режиме **Управление системой**.

Добавление индикаторов в Broadcom (Symantec) ProxySG

После экспорта индикаторов из Kaspersky CyberTrace файл с экспортированными индикаторами становится доступным для скачивания по следующему адресу:

`https://<CyberTrace_WebAddress>/ioc_exports/<iocexport_name>`

где `<iocexport_name>` – имя вашей задачи экспорта.

Чтобы добавить индикаторы в Broadcom (Symantec) ProxySG:

1. В интерфейсе Broadcom (Symantec) ProxySG выберите вкладку **Администратор**.

2. Выберите вкладку **Компактное представление**.

3. В разделе **Данные и облачные службы** выберите **Фильтрация контента**.

4. В открывшемся окне **Фильтрация содержимого** нажмите кнопку **Добавить локальную базу данных** над таблицей справа.

5. В разделе **Загрузка** окна **Добавить пользовательскую локальную базу данных** укажите URL для скачивания файла с экспортированными индикаторами.

Указывать имя пользователя и пароль (api_token) может не требоваться, если задача экспорта IoC из Kaspersky CyberTrace создана без базовой аутентификации.

Подробную информацию о добавлении индикаторов см. в аналогичном руководстве по добавлению потоков данных Kaspersky Network Security в Broadcom (Symantec) ProxySG.

Экспорт индикаторов в Security Code Continent NGFW

В этой статье описывается порядок интеграции Kaspersky CyberTrace с Security Code Continent NGFW, создания задачу экспорта индикаторов из Kaspersky CyberTrace и добавления индикаторов в Security Code Continent NGFW.

Security Code Continent NGFW – продукт для комплексной сетевой безопасности (UTM/NGFW) с поддержкой алгоритмов ГОСТ.

Создание задачи экспорта индикаторов из Kaspersky CyberTrace

В разделе **"Экспорт индикаторов"** вы можете создать или обновить задачу для предварительно заданных параметров экспорта индикаторов в Security Code Continent NGFW.

Чтобы создать задачу экспорта индикаторов из Kaspersky CyberTrace, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите в режим **Управление системой**.

2. Перейдите в раздел **Настройки** → **Экспорт индикаторов**.

3. В открывшемся окне **Экспорт индикаторов** нажмите на кнопку **Добавить задачу** и выберите **Security Code NGFW** в раскрывающемся списке.

4. В окне **Добавить задачу экспорта индикаторов** укажите следующие свойства:

   - В поле **Имя задачи** укажите уникальное имя задачи.
   - В поле **Экспортировать каждые** укажите частоту запуска задачи.
   - В поле **Максимальное количество записей** укажите количество экспортируемых индикаторов.
     Рекомендуемое количество индикаторов для одного экспорта (по умолчанию) составляет 50 000.
     Максимальное значение, которое можно указать – 1 000 000.
   - В поле **Тип файла** укажите тип файла.
     Тип файла – `.json`.
   - В поле **Тип индикатора** укажите тип индикатора.
     Доступные типы индикаторов: **IP-адрес**, **URL**, **домен**, **MD5**.

5. В разделах **Правила фильтрации** и **Условия сортировки** настройте фильтрацию и сортировку индикаторов.

6. Настройте ограничения доступа к файлу экспорта индикаторов.

   Для этого включите переключатель **Использовать авторизацию для загрузки отчета об экспорте индикаторов** и укажите имя пользователя и пароль.

7. Нажмите на кнопку **Next**.

8. В открывшемся окне **Предварительный просмотр экспорта** просмотрите файл экспорта.

9. Нажмите на кнопку **Add**.

Задача будет создана.

В окне **экспорта индикаторов** будет отображаться столбец с типом задачи экспорта. Если для задачи имеются предустановленные параметры, в столбце будет указано имя NGFW.

Предварительно установленная задача экспорта будет отображена в разделе **Задачи** в режиме **Управление системой**.

В разделе **"Экспорт индикаторов"** отображается ссылка на скачивание файла для предварительно установленной задачи экспорта.

Добавление индикаторов в Security Code Continent NGFW

После экспорта индикаторов из Kaspersky CyberTrace файл с экспортированными индикаторами становится доступным для скачивания по следующему адресу:

```
https://<CyberTrace_WebAddress>/ioc_exports/<iocexport_name>
```

где `<iocexport_name>` – имя вашей задачи экспорта.

Чтобы добавить индикаторы в Security Code Continent NGFW,

укажите URL для скачивания файла с экспортированными индикаторами в интерфейсе Security Code Continent NGFW.

Указывать имя пользователя и пароль (api_token) может не требоваться, если задача экспорта IoC из Kaspersky CyberTrace создана без базовой аутентификации.

Подробную информацию о добавлении индикаторов см. в документации Security Code Continent NGFW.

Копирование данных индикаторов в буфер обмена

На странице **"Индикаторы"** можно скопировать данные выбранных индикаторов в буфер обмена.

Чтобы скопировать данные индикаторов в буфер обмена:

1. Перейдите в режим "Управление данными".
2. Перейдите на страницу **"Индикаторы"**.
3. Выберите индикатор в таблице индикаторов.
4. На странице **"Сведения об индикаторе"** нажмите кнопку **"Копировать в буфер обмена"**.

   Данные индикатора будут скопированы в буфер обмена.

Пример скопированных данных индикатора выглядит следующим образом:


```
{
  "summary": {
    "type": "IP",
    "value": "3.171.57.166",
    "added_on": "Aug 13 2025 3:33 PM",
    "first_detected_on": "—",
    "last_detected_on": "—",
    "last_updated_on": "Aug 22 2025 3:32 PM",
    "false_positive": "—"
  },
  "suppliers": {
    "Demo_IP_Reputation_Data_Feed": {
      "confidence": 100,
      "type": "IP",
      "use_for_matching": true,
      "updated_on": "Aug 13 2025 3:33 PM",
      "category": "malware",
      "first_seen": "12.01.2025 04:30",
      "id": 61553062,
      "ip": "3.171.57.166",
      "ip_geo": "us",
      "ip_whois/created": "17.01.2024",
      "ip_whois/net_name": "AMAZON-CF",
      "ip_whois/net_range": "3.168.0.0 - 3.171.255.255",
      "ip_whois/updated": "17.01.2024",
      "last_seen": "10.08.2025 00:03",
      "popularity": 1,
      "threat_score": 60,
      "users_geo": "us, ar, co, ve"
    }
  },
  "internal_TI": {
    "confidence": 100,
    "type": "IP",
    "use_for_matching": true,
    "updated_on": "Aug 22 2025 3:32 PM",
    "attributes": {
      "attribute_one": "value_one",
      "attribute_three": "value_three",
      "attribute_two": "value_two",
      "Summary": "summary about of the indicator"
    }
  },
  "tags": {
    "critical_ip": "high",
    "us_ip": "medium"
  },
  "comments": {
    "author": {
      "text": "comment about of the indicator",
      "date": "Aug 22 2025 4:13 PM"
    }
  }
}
```

Правила нормализации URL

Различные вредоносные программы пытаются скрывать свою деятельность с помощью техник обфускации URL (например, с использованием национальных доменных имен, в том числе состоящих из одного символа; представления IP-адресов в восьмеричной записи; повторяющихся косых черт). В этом случае к одному и тому же контенту зачастую можно обращаться через формально разные адреса (например, адреса различающиеся схемой, портом или регистром символов в URL).

В результате при сопоставлении URL в их исходной форме со списками индикаторов компрометации (IoC) возникает проблема пропуска угроз, поскольку сопоставление с IoC оказывается безуспешным.

Например, github.com@520966948 — это скрытый IP-адрес 31.13.83.36, который на самом деле принадлежит facebook.com.

Kaspersky CyberTrace обеспечивает два преимущества:

- Нормализация URL, которая, как правило, отсутствует в SIEM-решениях.
- Маски, используемые в потоках данных об угрозах «Лаборатории Касперского» для закрытия групп вредоносных URL.

В потоках данных об угрозах «Лаборатории Касперского» невозможно было бы передавать тринадцать вариантов URL с разными вариантами нормализации, поскольку размер потока данных об угрозах был бы колоссальным. Однако, если пользователь будет отправлять нам известный URL в определенном формате, мы можем преобразовать его, сопоставить его с потоками данных об угрозах и обнаружить его с использованием нормализации.

> Для автоматизации нормализации URL-адресов в соответствии с приведенными ниже правилами можно использовать URL Normalizer — инструмент с открытым исходным кодом, созданный «Лабораторией Касперского».

На данный момент существует тринадцать правил нормализации URL-адресов. Ниже приведены примеры применения этих правил:

- Удаление сегментов-точек («`.`» и «`..`») в соответствии с алгоритмом, описанным в RFC 3986, раздел 5.2.4 «Удаление сегментов-точек» (https://www.ietf.org/rfc/rfc3986.txt):

  ```
  http://www.example.com/../a/b/../c/./d.html => http://www.example.com/a/b/c/d.html
  ```

- Удаление протокола:

  ```
  http://example.com => example.com
  ```

- Преобразование интернационализированных доменных имен в соответствии с алгоритмом Punycode, описанным в RFC 3492 (https://www.ietf.org/rfc/rfc3492.txt):

  ```
  тест.рф => xn--e1aybc.xn--p1ai
  ```

- Удаление префикса `www`:

  ```
  www.example.com => example.com
  ```

- Удаление повторяющихся косых черт:

  ```
  example.com//dir/test.html => example.com/dir/test.html
  ```

- Удаление косой черты в конце URL:

  `example.com/ => example.com`

- Удаление данных авторизации:

  `login:password@example.com => example.com`

- Удаление номера порта:

  `example.com:80/index => example.com/index`

- Удаление указания на фрагмент `#fragment`:

  `example.com#fragment => example.com`

- Удаление точек в конце имени хоста:

  `example.com./index.html => example.com/index.html`

- Преобразование символов, кодируемых знаком процента, в UTF-8 в соответствии с RFC 3986 (https://www.ietf.org/rfc/rfc3986.txt) and RFC 2279 (https://www.ietf.org/rfc/rfc2279.txt).

- Преобразование всех символов в нижний регистр:

  `EXAMPLE.COM => example.com`

- Преобразование IP-адреса (если указан), ведущего на запрашиваемый хост, в десятичную запись с точками:

  `0112.0175.0117.0150 => 74.125.79.104`

Для закрытия групп вредоносного URL в потоках данных об угрозах используются записи восьми типов, которые подразделяются на маскированные и немаскированные записи.

Сопоставление нормализованного URL с записями из баз данных на основе URL должно выполняться с учетом назначения определенных типов записей. Использование нормализации URL и масок обеспечивает увеличение количества обнаружений киберугроз для потока данных об угрозах, а также минимизирует объем передаваемых данных и снижает количество ложных срабатываний.

Подробные сведения приведены в руководстве «Kaspersky Threat Intelligence Data Feeds Implementation Guide».

Работа с ложными срабатываниями

Kaspersky CyberTrace позволяет отмечать индикаторы и связанные с ними обнаружения киберугроз как ложные срабатывания, просматривать индикаторы ложных срабатываний и связанные с ними обнаружения киберугроз на графе, а также отображать или скрывать ложные срабатывания в списках индикаторов, обнаружений киберугроз или на информационной панели.

Список ложных срабатываний проверяется только после сопоставления входящего события со всеми потоками данных об угрозах. Основное назначение списка ложных срабатываний заключается в возможности Kaspersky CyberTrace игнорировать срабатывания для доверенных индикаторов. Если какой-либо поток данных об угрозах выдает обнаружение киберугрозы, но соответствующий индикатор присутствует в списке ложных срабатываний, Kaspersky CyberTrace не генерирует оповещение об обнаружении индикаторов компрометации.

Если один и тот же индикатор добавлен в список пользовательских сведений о киберугрозах и в список ложных срабатываний, такой индикатор не игнорируется.

Отметка индикаторов как ложных срабатываний

На странице **Индикаторы** индикаторы можно отметить как ложные срабатывания. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Индикаторы можно отметить как ложные срабатывания следующими способами:

- В таблице индикаторов

  Здесь можно отметить как один индикатор, так и несколько индикаторов сразу.

- На странице определенного индикатора

Добавить индикаторы в список ложных срабатываний также можно вручную.

Чтобы отметить индикаторы как ложные срабатывания:

1. Выполните одно из следующих действий:

   - В столбце **Ложн** таблицы индикаторов нажмите на значок (**Нажмите, чтобы отметить индикатор как ложное срабатывание**) для индикатора, который требуется отметить.
   - В таблице индикаторов установите флажки рядом с индикаторами, которые требуется отметить.
   - В таблице индикаторов нажмите на значение требуемого индикатора.

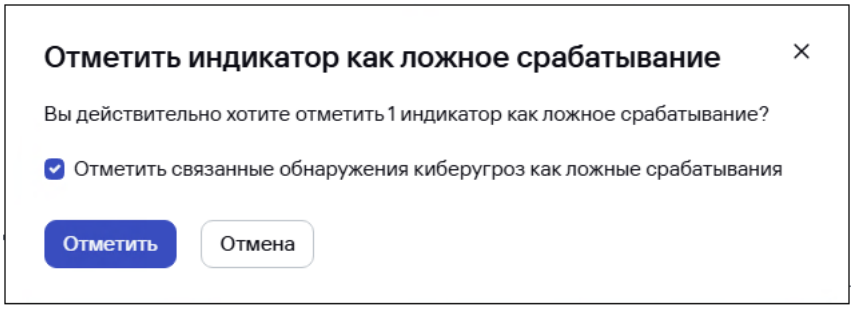
2. Выполните одно из следующих действий:

   - Если некоторые из выбранных индикаторов относятся к нескольким типам, выполните одно из следующих действий:
     - Нажмите кнопку **Ложное срабатывание**, затем нажмите кнопку **Отметить {{type}} как ложное срабатывание**, где **{{type}}** — тип индикатора, который требуется отметить как ложное срабатывание.
     - Нажмите кнопку **Ложное срабатывание**, затем нажмите **Отметить все как ложные срабатывания**, если требуется отметить индикаторы всех типов как ложные срабатывания.
   - Если ни один из выбранных индикаторов не относится к нескольким типам, нажмите кнопку **Отметить индикаторы**.

3. В открывшемся окне подтверждения выполните следующие действия:

   a. Если требуется отметить как ложные срабатывания и обнаружения киберугроз, связанные с индикаторами, оставьте установленным флажок **Отметить связанные обнаружения киберугроз как ложные срабатывания**.

   b. Нажмите на кнопку **Отметить**.



Подтверждение отметки индикатора как ложного срабатывания

Выбранные индикаторы отмечаются как ложные срабатывания. Если выбран этот вариант, соответствующие обнаружения киберугроз также отмечаются как ложные срабатывания.

Индикаторы, отмеченные как ложные срабатывания, отображаются со значком в столбце **Ложн** таблицы индикаторов.

Исключение индикаторов из списка ложных срабатываний

На странице **Индикаторы** можно исключить индикаторы из ложных срабатываний. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Индикаторы можно исключить из ложных срабатываний следующими способами:

- В таблице индикаторов

  Здесь можно исключить как один индикатор, так и несколько индикаторов сразу.

- На странице определенного индикатора

Исключить индикаторы из списка ложных срабатываний также можно вручную.

Чтобы исключить индикаторы из ложных срабатываний в таблице индикаторов:

1. Выполните одно из следующих действий:

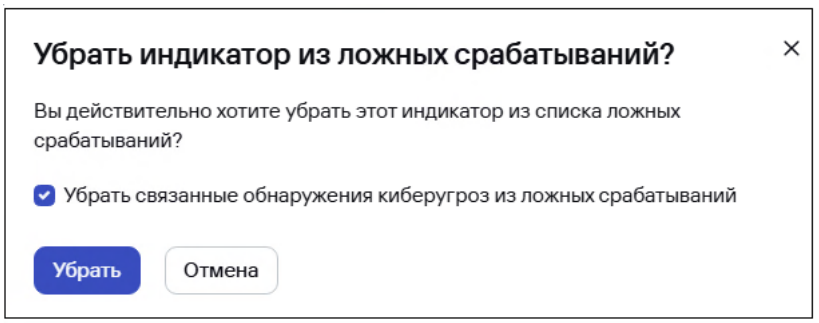
   - В столбце **Ложн** таблицы индикаторов нажмите на значок (**Нажмите для исключения индикатора из ложных срабатываний**) для индикатора, который требуется исключить.

   - В таблице индикаторов установите флажки рядом с требуемыми индикаторами и нажмите **Ложное срабатывание → Убрать индикаторы**.

2. В открывшемся окне подтверждения выполните следующие действия:

   a. Если требуется исключить из ложных срабатываний и связанные с индикаторами обнаружения, оставьте установленным флажок **Убрать связанные обнаружения киберугроз из ложных срабатываний**.

   b. Нажмите на кнопку **Убрать**.



Подтверждение исключения индикатора из ложных срабатываний

Выбранные индикаторы исключаются из ложных срабатываний. Если выбран этот вариант, соответствующие обнаружения киберугроз также исключаются из ложных срабатываний.

Индикаторы, не отмеченные как ложные срабатывания, отображаются со значком в столбце **Ложн** таблицы индикаторов.

Чтобы удалить индикатор из списка ложных срабатываний на странице этого индикатора, выполните следующие действия:

1. В таблице индикаторов нажмите на значение требуемого индикатора.

2. Выполните одно из следующих действий:

   - Если выбранный индикатор относится к нескольким типам, выполните одно из следующих действий:

     - Нажмите кнопку **Ложное срабатывание**, затем нажмите кнопку **Убрать {{type}} из ложных срабатываний**, где **{{type}}** — тип индикатора, который требуется убрать из ложных срабатываний.

     - Нажмите кнопку **Ложное срабатывание**, затем нажмите **Убрать все из ложных срабатываний**, если требуется исключить из ложных срабатываний индикаторы всех типов.

   - Если выбранный индикатор относится только к одному типу, нажмите **Убрать из ложных срабатываний**.

3. В открывшемся окне подтверждения выполните следующие действия:

   a. Если требуется исключить из ложных срабатываний и связанные с индикаторами обнаружения, оставьте установленным флажок **Убрать связанные обнаружения киберугроз из ложных срабатываний**.

   b. Нажмите на кнопку **Убрать**.

Индикатор исключается из ложных срабатываний. Если выбран этот вариант, соответствующие обнаружения киберугроз также исключаются из ложных срабатываний.

Индикаторы, не отмеченные как ложные срабатывания, отображаются со значком в столбце **Ложн** таблицы индикаторов.

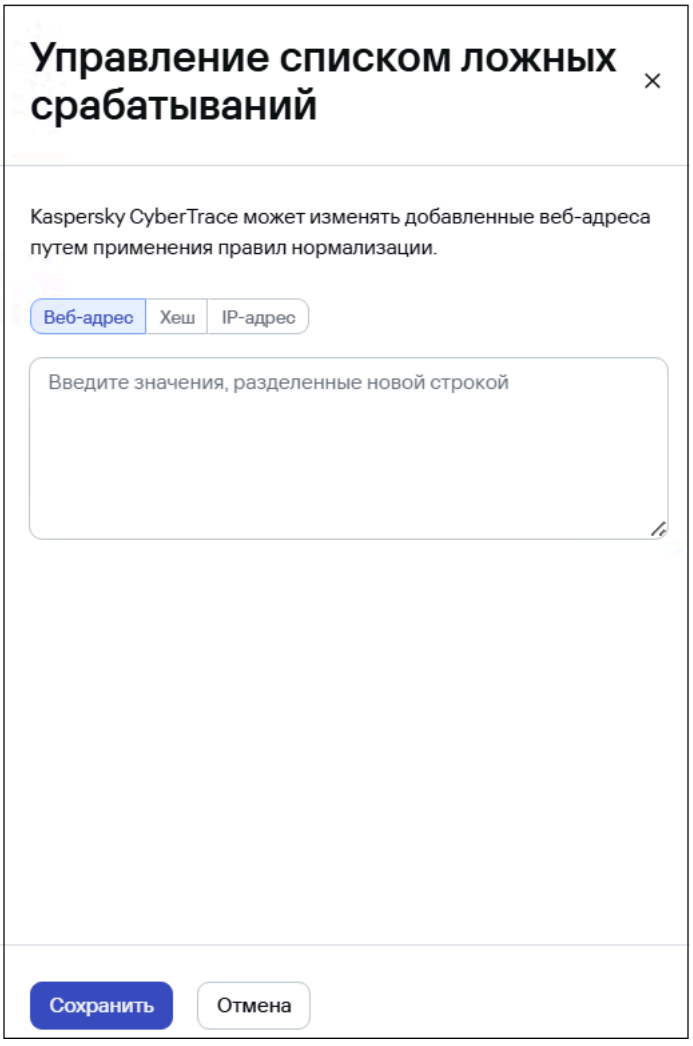
Работа с ложными срабатываниями

В этом разделе описывается порядок работы с со списком *Ложные срабатывания* на странице **Индикаторы**. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Порядок работы со списком ложных срабатываний:

1. Нажмите на кнопку **Управлять списком ложных срабатываний**.

   Откроется окно **Управление списком ложных срабатываний**:



Окно **Управление списком ложных срабатываний**

   В этом окне отображаются индикаторы, которые были отмечены как ложные срабатывания, и индикаторы, добавленные вручную, как описано в этом разделе.

2. Выберите вкладку **Веб-адрес**, **Хеш** или **IP-адрес**, чтобы открыть требуемую группу.

3. При необходимости добавьте или удалите индикаторы в выбранной группе.

   На вкладке **Веб-адрес** можно указать URL, содержащий подстановочный знак `*` (например, `example.com/testpage/*`, который будет сопоставляться с такими URL, как `example.com/testpage/test1` и `example.com/testpage/test/long_url`).

Kaspersky CyberTrace применяет правила нормализации URL ко всем добавляемым URL, которые еще не содержатся в базе данных индикаторов. Таким образом, представление того или иного URL может изменяться. Например, при добавлении URL, содержащего порт, значение порта удаляется.

Каждый индикатор в текстовом поле должен быть указан в отдельной строке.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Список ложных срабатываний обновлен.

Просмотр индикаторов и связанных с ними обнаруженных киберугроз, отмеченных как ложные срабатывания, на графе

Чтобы посмотреть на графе, отмечен ли индикатор или связанное с ним обнаружение как ложное срабатывание, выполните следующие действия:

1. На странице **Графы расследования** нажмите на граф, на котором требуется просмотреть индикаторы. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

2. Щелкните правой кнопкой мыши интересующий узел и выберите пункт **Показать сведения**.

   Справа откроется боковая панель, содержащая подробную информацию об узле.

3. Найдите строку **Ложное срабатывание**.

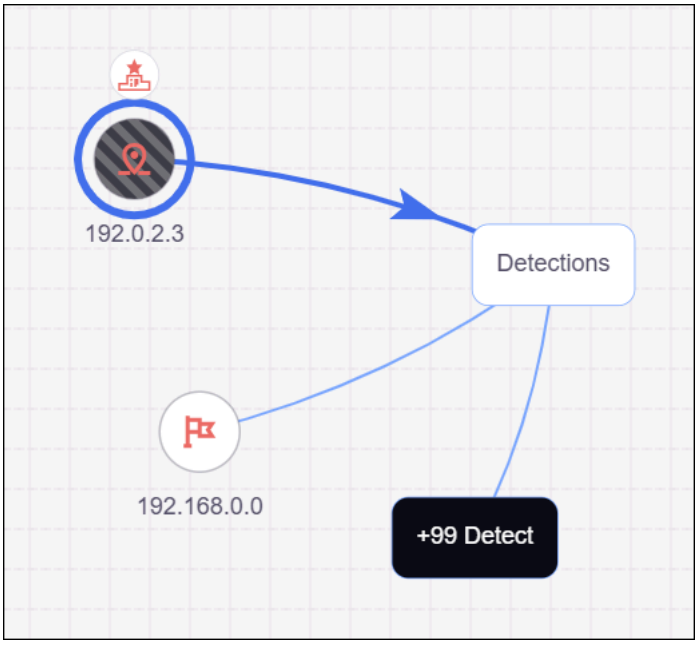
   У индикаторов, отмеченных как ложные срабатывания, указано значение **Да**.

   У индикаторов, отмеченных как ложные срабатывания, указано значение **Нет**.



Информация о ложных срабатываниях на графе

Индикаторы ложных срабатываний и соответствующие обнаруженные киберугрозы представлены на графе иначе, чем обычные индикаторы и обнаруженные киберугрозы (см. рисунок ниже):



Графическое представление ложных срабатываний на графе

Фильтрация ложных срабатываний и обнаружений киберугроз

При просмотре индикаторов или обнаружений киберугроз можно выполнять фильтрацию записей, отмеченных или не отмеченных как ложные срабатывания.

*Чтобы выбрать с помощью фильтра ложные срабатывания, которые будут отображаться на странице **Индикаторы**, выполните следующие действия:*

1. Нажмите на значок (воронка) в столбце **Ложн** таблицы.
2. В открывшемся диалоговом окне выберите один из вариантов:
   - **Ложные срабатывания**
   - **Не ложные срабатывания**

   В таблице отображаются выбранные записи.

*Чтобы выбрать с помощью фильтра ложные срабатывания, которые будут отображаться на странице **Обнаружения**, выполните следующие действия:*

1. Нажмите на значок (воронка) в столбце **Дополнительная информация** таблицы.
2. В открывшемся диалоговом окне выберите **Все**, **Ложные срабатывания** или **Не ложные срабатывания**.

   В таблице отображаются выбранные записи.

Отображение статистики по ложным срабатываниям на информационной панели

Отображение статистики по ложным срабатываниям *на странице* ***Информационная панель***

1. Нажмите на значок ⚙ (**Настроить информационную панель**).
2. Включите переключатель **Показывать ложные срабатывания**.

В результате статистика ложных срабатываний отображается на виджетах **Статистика сопоставлений** и **Статистика по потокам индикаторов**, а также на пользовательских виджетах.

Использование графов

Графы позволяют визуализировать информацию об индикаторах угроз и их взаимосвязях, обнаруженных киберугрозах, отчетах и т. д. Помимо информации из Kaspersky CyberTrace, граф можно обогатить информацией из внешних источников, таких как Kaspersky Threat Intelligence Portal и VirusTotal.

Из-за ограничений, налагаемых уровнем лицензирования, эта функция может быть отключена.

Работа с графами

Страница **Графы расследования** веб-интерфейса Kaspersky CyberTrace позволяет работать с графами. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

С графами можно выполнять следующие действия:

- Создание нового графа.

  Графы также можно создавать на странице **Индикаторы** или **Обнаружения** (см. инструкцию далее в этом разделе).

- Просмотр существующего графа нажатием на его плитку.
- Для работы с существующим графом используется его меню, вызываемое кнопкой ⋮ (вертикальное многоточие):
  - Создание копию графа.
  - Получение ссылки на страницу графа, которую можно кому-нибудь отправить.
  - Экспорт графа в CSV.
  - Удаление графа.

- Измените имя и описание графа, нажав на кнопку (**Изменить граф**).
- Отсортируйте список графов, выбрав критерий сортировки (**Дата доступа**, **Название**, **Автор**, **Дата создания** или **Дата изменения**) и порядок (**По возрастанию** или **По убыванию**).

Создание графа

Чтобы создать новый граф, выполните следующие действия:

1. На странице **Графы расследования** нажмите на кнопку **Добавить граф**.

   Откроется новый граф.

2. Внесите в граф необходимые изменения.
3. Нажмите на кнопку (**Сохранить**).

   Откроется диалоговое окно **Сохранить граф**.

4. В поле **Название** введите имя графа.
5. В поле **Описание** введите описание графа.
6. Нажмите на кнопку **Сохранить**.

Создание графа на странице индикаторов

Чтобы создать граф на странице индикаторов, выполните следующие действия:

1. На странице **Индикаторы** нажмите на значение индикатора, который требуется добавить на граф.

   Откроется страница **Сведения об индикаторе**.

2. Нажмите на кнопку **Показать на графе**.

Kaspersky CyberTrace создаст новый граф, содержащий узел индикатора.

Создание графа на странице обнаружений киберугроз

Чтобы создать граф на странице обнаружений киберугроз, выполните следующие действия:

1. На вкладке **Обнаружения** выберите обнаружение киберугрозы, которое требуется добавить на граф.

   Откроется страница **Сведения об обнаружении киберугрозы**.

2. Нажмите на кнопку **Показать на графе**.

Kaspersky CyberTrace создаст новый граф, содержащий узел обнаружения киберугрозы.

Об узлах и связях

Каждый граф состоит из узлов (индикаторов, обнаруженных киберугроз и т. д.) и связей, соединяющих узлы. Как узлы, так и связи могут добавляться на граф вручную или в результате трансформации.

Узлы

Узел представляет собой отдельную точку на графе, которая может быть связана с другими точками. Существуют различные типы узлов, такие как индикаторы, обнаруженные киберугрозы или группы. Узлы разных типов отображаются на графе разными символами. Описание различных типов узлов приведено в таблице ниже.

Типы узлов

Значок	Type	Описание
	Веб-адрес	Стандартные индикаторы Kaspersky CyberTrace.
	Хеш	
	IP-адрес	
	External URL	Внешний индикатор (наблюдаемый объект), полученный из любого источника кроме базы данных Kaspersky CyberTrace.
	Внешний хеш	Граф может содержать внешний индикатор и стандартный индикатор Kaspersky CyberTrace, которые имеют одинаковое значение.
	Внешний IP-адрес	
	Действие/обнаружения киберугроз	Промежуточный узел между другими узлами. Этот промежуточный узел возникает в результате трансформации.
	Обнаружение	Оповещение об обнаружении индикаторов компрометации.
	Отчет	Отчет, содержащий информацию о соответствующем индикаторе.
	Группа	Несколько узлов, сгруппированных вместе.

Связи

Узлы соединяются друг с другом *связями*. Связи могут быть *ориентированными* или *неориентированными*.

Ориентированная связь может вести только к узлам типов «Действие» и «Обнаруженные киберугрозы». Такая связь возникает, когда Kaspersky CyberTrace выполняет трансформацию, и новая связь ведет от исходного узла к узлу, добавленному после трансформации.

Например, если пользователь запускает трансформацию, чтобы найти обнаруженные киберугрозы, связанные с индикатором, может возникнуть ориентированная связь, ведущая от данного индикатора к узлу типа «Обнаруженные киберугрозы». В свою очередь, неориентированные связи соединяют новый узел «Обнаруженные киберугрозы» с узлами типа «Обнаруженные киберугрозы.

В большинстве случаев *неориентированная* связь соединяет два узла, у которых есть нечто общее.

Например, опасный файл может иметь разные хеши (MD5, SHA1 и SHA256), каждый из них при этом является отдельным индикатором угрозы. Все эти узлы могут быть соединены неориентированными связями.

Неориентированные связи можно создавать вручную, тогда как ориентированные связи могут быть только результатом трансформации.

Работа с узлами и связями

Для управления узлами и связями графа выполните следующие действия:

На странице **Графы расследования** нажмите на плитку графа, чтобы открыть его.

Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Добавление узлов в граф

Узлы можно добавлять в граф следующими способами:

- Добавление узлов типа «Индикатор» или «Обнаруженные киберугрозы» при создании графа на страницах **Индикаторы** или **Обнаружения** соответственно.
- Добавление узлов типа «Стандартный индикатор Kaspersky CyberTrace» и «Внешний индикатор (наблюдаемый объект)» в существующий граф вручную или из файлов.
- Добавление узлов в существующий граф с помощью трансформаций.

Чтобы добавить узел в существующий граф вручную, выполните следующие действия:

1. Нажмите на кнопку + (**Добавить индикаторы**) на боковой панели.
2. В открывшемся диалоговом окне **Добавление индикаторов на граф** укажите значение индикатора, который требуется добавить. Например, MD5-хеш файла или URL-адрес.

   Если в базе данных Kaspersky CyberTrace имеется информация об указанном значении, Kaspersky CyberTrace предлагает выбрать, требуется ли добавить это значение из базы данных в качестве стандартного индикатора Kaspersky CyberTrace или добавить внешний индикатор (наблюдаемый объект).

   Если в базе данных Kaspersky CyberTrace отсутствует информация об указанном значении, можно добавить только внешний индикатор (наблюдаемый объект).

   Также можно указать несколько значений одно за другим.
3. Нажмите на кнопку **Создать узлы**.

Добавленные узлы появятся в графе.

Если узел уже существует в графе:

- Индикатор Kaspersky CyberTrace обновляется из базы данных.
- Внешний индикатор (наблюдаемый объект) остается на графе, а новые узлы не добавляются.

Чтобы добавить узел к существующему графу из файла, выполните следующие действия:

1. Нажмите на кнопку + (**Добавить индикаторы**) на боковой панели.
2. В открывшемся диалоговом окне **Добавление индикаторов на граф** перейдите на вкладку **Из файлов**.
3. Выполните одно из следующих действий:
   - Перетащите требуемый файл (файлы) в область диалогового окна.
   - Нажмите на кнопку **Добавить файлы** и выберите требуемый файл или файлы из папки.

   Добавить можно только текстовые файлы в кодировке UTF-8 без BOM (размер каждого файла до 128 КБ). Файл можно удалить перед добавлением.
4. Нажмите на кнопку **Создать узлы**.

Добавленные узлы появятся в графе.

Если узел уже существует в графе:

- Индикатор Kaspersky CyberTrace обновляется из базы данных.
- Внешний индикатор (наблюдаемый объект) остается на графе, а новые узлы не добавляются.

Просмотр информации об узлах

Подробную информацию можно просмотреть о следующих типах узлов:

- Стандартный индикатор Kaspersky CyberTrace:
  - Тип и значение индикатора.
  - Ссылка на страницу индикатора в веб-интерфейсе Kaspersky CyberTrace.
  - Дата и время, когда индикатор был добавлен в граф.
  - Дата и время первого и последнего обнаружения киберугроз.
  - Источники индикатора.
  - Контекст индикатора.
  - Был ли индикатор отмечен как ложное срабатывание.

- Внешний индикатор (наблюдаемый объект):
  - Тип и значение индикатора.
  - Ссылка на внешний источник индикатора, если есть.
  - Дата и время, когда индикатор был добавлен в граф.
  - Атрибуты индикатора, если есть.
- Обнаружение киберугрозы:
  - Дата и время обнаружения киберугрозы.
  - Дата и время, когда обнаружение киберугрозы было добавлено в граф.
  - Категория обнаружения киберугрозы.
  - Имя тенанта, для которого было получено обнаружение киберугрозы, если существуют тенанты кроме «General».
  - Имя источника событий.
  - Входящее событие.
  - Части входящего события (в формате «ключ-значение»), которые были получены из регулярных выражений, примененных к входящему событию, и имена этих регулярных выражений.
  - События, включающие данное обнаружение киберугрозы.
  - Части оповещения об обнаружении индикаторов компрометации обнаружений киберугроз (в формате «ключ-значение»), соответствующие контексту обнаруженного индикатора.
  - Стандартный индикатор Kaspersky CyberTrace, вызвавший обнаружение киберугрозы.
- Отчет
  - Дата и время, когда отчет был добавлен в граф.
  - Имя отчета.
  - Поставщик отчета.
  - Тип отчета, если есть.
  - Ссылка на отчет, если есть.

Чтобы просмотреть подробную информацию об узле:

1. Щелкните правой кнопкой мыши интересующий узел.
2. В контекстном меню выберите команду **Показать сведения**.

Справа откроется боковая панель, содержащая подробную информацию об узле.

Также можно просмотреть информацию об узлах в группе.

Создание связей путем соединения узлов

Связь между узлами можно создать следующими способами:

- Соединение узлов вручную в режиме связывания.
- Автоматическое создание связей с помощью трансформаций.

Чтобы соединить узлы вручную, выполните следующие действия:

1. Включите режим связывания, для этого нажмите на кнопку (**Режим связывания**) на боковой панели.
2. Щелкните по узлу, который требуется соединить с другим узлом.

   На графе создается соединительная линия, ведущая от начального узла к следующему выбранному узлу.
3. Щелкните по следующему узлу, чтобы создать связь.

Когда соединение узлов будет закончено, отключите режим связывания.

Удаление узлов

Чтобы удалить узел, выполните следующие действия:

1. Выберите узел, который требуется удалить.
2. Нажмите на кнопку (**Удалить узлы**) на боковой панели или нажмите клавишу **DEL** на клавиатуре.

   Вместо этого можно щелкнуть правой кнопкой мыши по требуемому узлу и выбрать в контекстном меню команду **Удалить узел**.
3. В открывшемся окне подтверждения нажмите кнопку **Удалить** для подтверждения удаления узла.

При удалении узлов следует учитывать следующие соображения:

- При удалении узла группы удаляются все узлы в этой группе. Вместо удаления узла группы можно разгруппировать его или удалить отдельные узлы в группе.
- В случае удаления узла, соединенного с узлом «Действие» или «Обнаруженные киберугрозы» ориентированной связью, Kaspersky CyberTrace удаляет как исходный узел, так и узел «Действие» или «Обнаруженные киберугрозы». Если существуют другие узлы, связанные с узлом «Действие» или «Обнаруженные киберугрозы» неориентированными связями, Kaspersky CyberTrace не удаляет эти узлы.

Удаление связей

При удалении узла Kaspersky CyberTrace автоматически удаляет связи, соединяющие этот узел с другими узлами графа. Связи также можно удалять вручную, не удаляя при этом сами узлы.

Чтобы удалить связь, выполните следующие действия:

1. Щелкните по связи правой кнопкой мыши.
2. В контекстном меню нажмите **Удалить связь**.

О трансформациях

Помимо добавления узлов и связей в граф вручную, Kaspersky CyberTrace может обогащать граф автоматически путем добавления информации об объектах, имеющих отношение к узлу. Источником этой информации может быть как собственно Kaspersky CyberTrace, так и внешние источники, такие как Kaspersky Threat Intelligence Portal или VirusTotal. Выполнение процесса обогащения графа называется *трансформацией*.

Большинство источников обогащения графов не поддерживают обработку индикаторов URL, содержащих символ «*» в доменной части. Выполнение трансформации на узле с таким индикатором URL приведет к ошибке или пустому результату.

По умолчанию Kaspersky CyberTrace предоставляет следующие трансформации:

- **Связанные индикаторы CyberTrace**

  Получение индикаторов из тех же потоков данных с первоначальным стандартным индикатором Kaspersky CyberTrace:

  - **Индикаторы IP**
  - **Индикаторы хешей**
  - **Индикаторы веб-адресов**
  - **Все индикаторы**

    Все связанные индикаторы (хеши, URL, IP-адреса).

- **Связанные обнаружения киберугроз CyberTrace**

  Получение 100 последних обнаружений киберугроз, связанных со стандартным индикатором Kaspersky CyberTrace.

- Получение информации от Kaspersky Threat Intelligence Portal.

  Kaspersky CyberTrace необходим токен доступа для подключения к Kaspersky Threat Intelligence Portal.

  - Для индикаторов типа URL (стандартные индикаторы Kaspersky CyberTrace, а также внешние индикаторы (наблюдаемые объекты)) Kaspersky CyberTrace может получить следующую информацию:
    - **Файлы, обращавшиеся к веб-адресу**
    - **Файлы, скачанные с веб-адреса**
    - **Веб-адрес, ссылающиеся на веб-адрес**

- **Веб-адреса, на которые ссылается веб-адрес**
- **Разрешения DNS с веб-адреса**

  IP-адреса из разрешения DNS для данного URL.
- **Отчеты для веб-адреса**

- Для индикаторов типа MD5, SHA1 и SHA256 (стандартные индикаторы Kaspersky CyberTrace, а также внешние индикаторы (наблюдаемые объекты)) Kaspersky CyberTrace может получить следующую информацию:
  - **Файлы, запускающие файл**
  - **Файлы, запускаемые файлом**
  - **Файлы, скачивающие файл**
  - **Файлы, скачиваемые файлом**
  - **Веб-адреса, к которым обращается файл**
  - **Веб-адреса, по которым расположен файл**
  - **Отчеты для файла**
- Для индикаторов типа IP (стандартные индикаторы Kaspersky CyberTrace, а также внешние индикаторы (наблюдаемые объекты)) Kaspersky CyberTrace может получить следующую информацию:
  - **Файлы, скачанные с IP-адреса**
  - **Веб-адреса, связанные с IP-адресом**
  - **Отчеты для IP-адреса**

- Получение информации от VirusTotal.

  Kaspersky CyberTrace необходим токен доступа для подключения к VirusTotal.

  - Для индикаторов типа URL (стандартные индикаторы Kaspersky CyberTrace, а также внешние индикаторы (наблюдаемые объекты)) Kaspersky CyberTrace может получить следующую информацию:
    - **Получить информацию VirusTotal**

      Информация о данном URL.
    - **Файлы, обменивающиеся данными**

      Список файлов, которые взаимодействуют с данным URL.
    - **Скачанные файлы**

      Список файлов, загруженных с данного URL.
    - **Содержащие файлы**

      Список файлов, содержащих указанный URL.

- **Домены, к которым были обращения**

  Список доменов, с которых данный URL загружает какой-либо ресурс.

- **Веб-адрес, ссылающиеся на веб-адрес**

  Список URL, ссылающихся на данный URL.

- **Перенаправляющие веб-адреса**

  Список URL, на которые перенаправляет данный URL.

- **Перенаправляемые веб-адреса**

  Список URL, перенаправляющих на данный URL.

- **Поддомены**

  Список поддоменов для данного домена.

  При таких трансформациях перед отправкой запроса в API VirusTotal Kaspersky CyberTrace определяет, действительно ли целевой узел определенно является доменом.

  Если узел является не «чистым» доменом, а URL, возвращается пустой результат.

- **Веб-адреса домена**

  Список URL для данного домена.

  Перед отправкой запроса в API VirusTotal Kaspersky CyberTrace определяет, действительно ли целевой узел определенно является доменом. Если узел является не «чистым» доменом, а URL, возвращается пустой результат.

- **IP-адреса, к которым были обращения**

  Список IP-адресов, с которых данный URL загружает какой-либо ресурс.

- **Последнее разрешение IP-адреса**

  Последнее разрешение IP-адреса для данного URL.

- **Сетевое местоположение**

  Сетевое местоположение для данного URL.

- **Разрешения домена**

  Список IP-адресов, на которые разрешается данный домен.

  Перед отправкой запроса в API VirusTotal Kaspersky CyberTrace определяет, действительно ли целевой узел определенно является доменом. Если узел является не «чистым» доменом, а URL, возвращается пустой результат.

- Для индикаторов типа MD5, SHA1 и SHA256 (стандартные индикаторы Kaspersky CyberTrace, а также внешние индикаторы (наблюдаемые объекты)) Kaspersky CyberTrace может получить следующую информацию:

  - **Получить информацию VirusTotal**

    Информация о данном хеше.

  - **Файлы из одного архива**

    Список файлов, входящих в тот же архив, что и файл с данным хешем.

- **Carbon Black: дочерние**

  Список файлов, которые являются дочерними по отношению к файлу с данным хешем.

- **Carbon Black: родительские**

  Список файлов, которые являются родительскими по отношению к файлу с данным хешем.

- **Сжатые: родительские**

  Список файлов (архивов), содержащих файл с данным хешем.

- **Отброшенные файлы**

  Список файлов, которые удалил файл с данным хешем.

- **Файлы, исполнявшие файл**

  Список файлов, запускавших файл с данным хешем.

- **Домены, к которым были обращения**

  Список доменов, к которым обращался файл с данным хешем.

- **Веб-адреса с обращениями**

  Список URL, к которым обращался файл с данным хешем.

- **Встроенные IP-адреса**

  Список IP-адресов, встроенных в файл с данным хешем.

- **Встроенные веб-адреса**

  Список URL, встроенных в файл с данным хешем.

- **Доменные имена In the wild**

  Список доменов, с которых был загружен файл с данным хешем.

- **Веб-адреса In the wild**

  Список URL, с которых был загружен файл с данным хешем.

- **IP-адреса, к которым были обращения**

  Список IP-адресов, к которым обращался файл с данным хешем.

- **IP-адреса In the wild**

  Список IP-адресов, с которых был загружен файл с данным хешем.

- Для индикаторов типа IP (стандартные индикаторы Kaspersky CyberTrace, а также внешние индикаторы (наблюдаемые объекты)) Kaspersky CyberTrace может получить следующую информацию:

  - **Получить информацию VirusTotal**

    Информация о данном IP-адресе.

  - **Файлы, обменивающиеся данными**

    Список файлов, которые взаимодействуют с данным IP-адресом.

  - **Скачанные файлы**

    Список файлов, загруженных с данного IP-адреса.

- **Содержащие файлы**

  Список файлов, содержащих данный IP-адрес.

- **Разрешение IP-адресов**

  Список доменов, которые разрешаются на данный IP-адрес.

- **Веб-адреса для IP-адреса**

  Список URL, ведущих на данный IP-адрес.

Выполнение трансформаций

Чтобы трансформировать узел, выполните следующие действия:

1. На странице **Графы расследования** нажмите на плитку графа, чтобы открыть его.

   Для работы с этой страницей необходимо перейти в режим **Управление данными**.

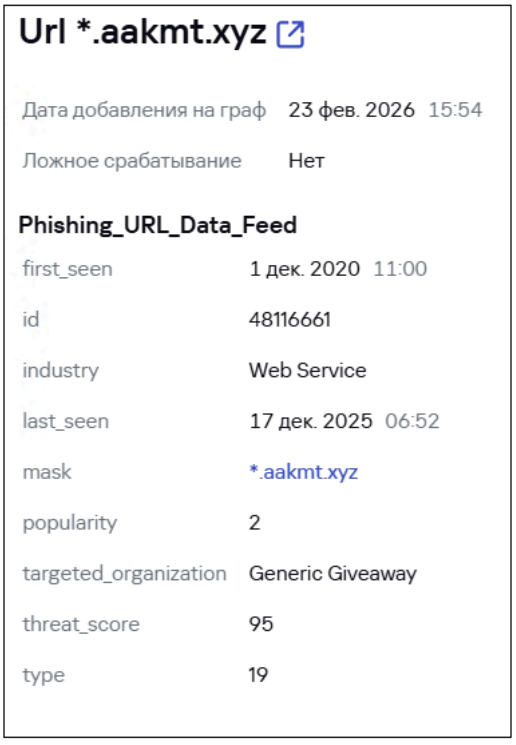
2. Щелкните по узлу правой кнопкой мыши.

3. В контекстном меню выберите трансформацию, которую требуется выполнить. Контекстное меню узла включает только те трансформации, которые доступны для данного узла.

   Если источник обогащения графа содержит требуемую информацию, то после завершения трансформации на графе появятся новые узлы и связи.

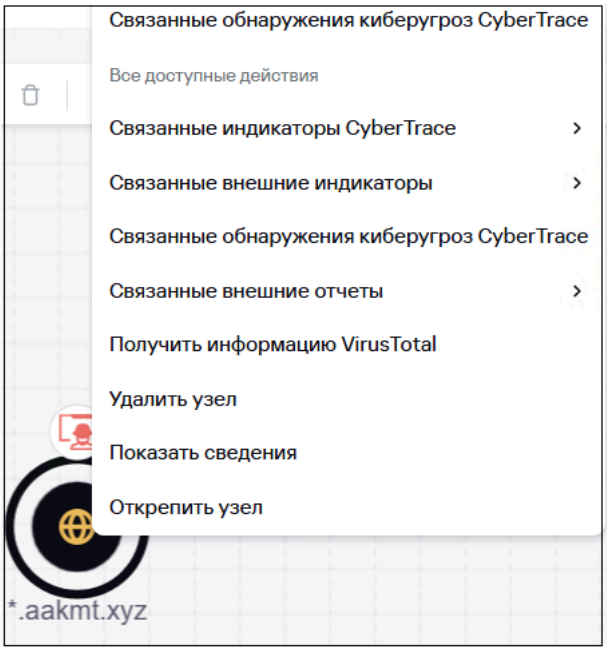
В результате трансформации полученный граф объединяется с текущим графом.

На боковой панели для узла типа «внешний индикатор» и «индикатор Kaspersky CyberTrace» отображается вся контекстная информация об узле, в том числе результаты внешних источников (если они присутствуют в трансформации).



Боковая панель с контекстной информацией узла

Также можно вызвать три последние трансформации, выполненных для данного графа. Такие трансформации отображаются в контекстном меню узла.



Вызов последних трансформаций в контекстном меню

Во время трансформации недоступны следующие возможности:

- Добавление новых узлов в граф.
- Отмена и повторение действий.
- Использование режима связывания.
- Сохранение графа.
- Копирование ссылки на граф.
- Экспорт графа.
- Открытие контекстного меню узла.
- Запуск новой трансформации.

Одновременно выполнять трансформацию для нескольких узлов невозможно.

Группы узлов

Для более компактного представления узлы графа можно объединять в *группы*. Группа представлена в графе особым узлом, отдельные узлы, входящие в группу, скрываются.

Для управления группами узлов графа выполните следующие действия:

На странице **Графы расследования** нажмите на плитку графа, чтобы открыть его.

Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Чтобы сформировать группу, узлы должны удовлетворять следующим требованиям:

- Все узлы должны иметь один и тот же тип.

  В группу можно объединить узлы следующих типов:

  - стандартный индикатор Kaspersky CyberTrace;
  - внешний индикатор (наблюдаемый объект);
  - обнаружение киберугрозы;
  - отчет.

- Каждый узел связан с *родительским узлом группы*, причем это единственная связь данного узла.

Узлы можно группировать вручную или настроить граф так, чтобы узлы группировались автоматически средствами Kaspersky CyberTrace.

Группирование узлов вручную

Узлы можно сгруппировать вручную, если они удовлетворяют требованиям, описанным выше.

Чтобы сгруппировать узлы вручную, выполните следующие действия:

1. Выберите несколько узлов, которые требуется сгруппировать. Для этого удерживайте клавишу **CTRL** и нажимайте на требуемые узлы.
2. Щелкните правой кнопкой мыши по любому выбранному узлу и выберите команду **Добавить выбранные узлы в групповой узел**.

Выбранные узлы заменяются единым узлом, отображающим количество узлов в группе и их тип.

Добавление узлов в существующую группу

Узлы можно добавить в существующую группу, если эти узлы имеют тот же тип, что и узлы в данной группе, и тот же самый родительский узел.

Чтобы добавить узел в существующую группу, выполните следующие действия:

1. Выберите добавляемый узел и группу.

   Также можно выбрать для добавления сразу несколько узлов.

2. Щелкните правой кнопкой мыши по любому выбранному узлу и выберите команду **Добавить выбранные узлы в групповой узел**.

Автоматическое группирование

Граф можно настроить так, чтобы узлы группировались в Kaspersky CyberTrace автоматически.

Чтобы настроить автоматическое группирование, выполните следующие действия:

1. На странице графа нажмите на кнопку ⚙ (**Настройка графа**).
2. В окне **Настройка графа** перейдите на вкладку **Группы**.
3. Установите переключатель в положение **Автоматическое группирование включено**.
4. Укажите минимальное количество узлов для группирования.
5. Нажмите на кнопку **Сохранить**.
6. Сохраните граф, если новые параметры должны применяться на постоянной основе. В противном случае настройки будут сброшены после завершения работы с графом.

Группа будет автоматически сформирована, если количество узлов, соответствующих перечисленным выше требованиям, станет равно или больше, чем указано в настройках автоматического группирования.

Панель группы

По двойному щелчку по узлу группы отображается панель, содержащая информацию об узлах, входящих в группу, в виде таблицы.

На панели группы можно выполнить следующие действия:

- Поиск узлов с помощью поля поиска в верхней части панели.
- Фильтрация таблицы с помощью формы фильтра, которая отображается по нажатию на значок ▽ (воронка) в заголовке столбца.
- Исключение выбранных узлов из группы с помощью кнопки **Убрать из группового узла**.
- Удаление выбранных узлов с помощью кнопки **Удалить**. При удалении узла в группе этот узел полностью удаляется из графа.

Фильтрация и поиск

Чтобы отфильтровать узлы графа или выполнить их поиск, выполните следующие действия:

На странице **Графы расследования** нажмите на плитку графа, чтобы открыть его.

Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Фильтрация узлов

Чтобы отфильтровать узлы, выполните следующие действия:

1. Нажмите на кнопку (**Фильтры графа**) на верхней панели инструментов.

   Откроется форма фильтра.

2. Укажите правила фильтрации для узлов, которые должны быть показаны на графе. Например, чтобы отобразить только узлы определенного типа:

   a. Нажмите на кнопку **Тип узла**.

      Появится фильтр **Тип узла**.

   b. Установите флажки для типов узлов, которые требуется отображать на графе. Например, «Наблюдаемый объект».

   c. Нажмите на кнопку **Применить**.

   На графе отобразятся только узлы типа «Наблюдаемый объект» и их связи.

   > Если указано несколько фильтров, граф будет содержать только те узлы и связи, которые удовлетворяют всем условиям фильтрации.

3. Если фильтр должен применяться на постоянной основе, граф необходимо сохранить.

В таблице ниже перечислены фильтры, которые можно использовать для фильтрации узлов.

Фильтры для графа

Фильтр	Описание
Тип узла	Укажите типы узлов для отображения на графе. Можно выбрать следующие типы узлов: • Стандартный индикатор Kaspersky CyberTrace • Внешний индикатор (наблюдаемый объект) • Обнаружение • Отчет • Группа узлов Можно выбрать несколько вариантов одновременно.
Тип индикатора	Укажите, какие типы индикаторов требуется отображать на графе. Этот фильтр можно применить к следующим типам узлов: • Стандартный индикатор Kaspersky CyberTrace • Внешний индикатор (наблюдаемый объект) • Группа узлов, содержащая индикаторы Можно выбрать несколько вариантов одновременно.
Значение индикатора	Укажите подстроку для поиска по значениям индикаторов. Этот фильтр можно применить к следующим типам узлов: • Стандартный индикатор Kaspersky CyberTrace • Внешний индикатор (наблюдаемый объект) • Группа узлов, содержащая индикаторы

Фильтр	Описание
Контекст индикатора	Условия фильтрации индикаторов по значениям атрибутов индикатора. В раскрывающемся меню выберите поле контекста, затем укажите его значение, чтобы отображались только те индикаторы, у которых есть указанное поле контекста и значение. Можно выбрать несколько вариантов одновременно. Этот фильтр можно применить к следующим типам узлов: • Стандартный индикатор Kaspersky CyberTrace • Группа узлов, содержащая стандартные индикаторы Kaspersky CyberTrace
Контекст обнаружения киберугрозы	Условия фильтрации обнаружений киберугроз по значениям атрибутов обнаружения киберугрозы. Kaspersky CyberTrace извлекает эти атрибуты из поступающих событий с помощью регулярных выражений. В раскрывающемся меню выберите имя регулярного выражения, затем укажите его значение, чтобы отображались только те обнаружения киберугроз, у которых есть указанное поле контекста и значение. Можно выбрать несколько вариантов одновременно. Этот фильтр можно применить к следующим типам узлов: • Обнаруженные киберугрозы • Группа узлов, содержащая обнаружения киберугроз

Поиск узлов

Чтобы выполнить поиск определенного узла, выполните следующие действия:

Введите поисковый запрос в поле поиска в верхней части графа.

Результаты поиска выводятся под полем поиска. Нажмите на узел в списке результатов, чтобы найти узел на графе.

Изменение размера графа и полноэкранный режим

Чтобы изменить размер графа или перейти в полноэкранный режим, выполните следующие действия:

1. На странице **Графы расследования** нажмите на плитку графа, чтобы открыть его.

   Для работы с этой страницей необходимо перейти в режим **Управление данными**.

2. Наведите указатель мыши на значок **100%** в нижней части графа.

   Появится полоса изменения размера:

3. Чтобы перейти в полноэкранный режим, нажмите на значок . Чтобы выйти из полноэкранного режима, нажмите на значок или нажмите клавишу **ESC**.

4. Чтобы изменить размер графа, нажмите на значок (увеличить) или (уменьшить).

   Изменить размер графа также можно прокруткой колесом мыши или сочетаниями клавиши **CTRL** с клавишами «**+**» (плюс) или «**-**» (минус).

Экспорт информации из графа

Информацию обо всех индикаторах на графе можно экспортировать в файл CSV.

Чтобы экспортировать информацию об индикаторах, выполните следующие действия:

1. На странице **Графы расследования** нажмите на плитку графа, чтобы открыть его.

   Для работы с этой страницей необходимо перейти в режим **Управление данными**.

2. Нажмите на кнопку (**Экспортировать в CSV**) в верхнем меню.

3. Укажите путь и имя CSV-файла.

4. Сохраните файл.

Формат экспортируемого файла

Столбец	Описание
`type`	Тип индикатора. Возможные значения: • `URL` • `IP` • `MD5` • `SHA1` • `SHA256`
`value`	Значение индикатора.
`is_observable`	Двоичный флаг, указывающий, был ли индикатор добавлен из внешнего источника или присутствовал в базе Kaspersky CyberTrace: • `TRUE` — индикатор был добавлен из внешнего источника. • `FALSE` — индикатор присутствовал в базе Kaspersky CyberTrace.
`is_false_positive`	Двоичный флаг, указывающий, принадлежит ли индикатор к источнику данных об угрозах `FalsePositive`: • `TRUE` — индикатор принадлежит к источнику данных об угрозах `FalsePositive`. • `FALSE` — индикатор не принадлежит к источнику данных об угрозах `FalsePositive`.
`created_date`	Дата и время, когда индикатор был добавлен в граф.
`updated_date`	Дата и время обновления информации об индикаторе.

Использование тегов

Индикаторам можно назначать категорию и приоритет с помощью *тегов*. Сами теги похожи на пользовательские категории: один и тот же тег можно назначить разным индикаторам, если у них есть что-то общее. Одному индикатору можно присвоить несколько тегов.

У каждого тега есть показатель важности или *вес тега*. С его помощью можно управлять приоритетами индикаторов. Соответствие между важностью тега и весом тега показано в таблице ниже.

Соответствие между важностью тега и весом тега

Важность тега	Вес тега
Нет	0
Незначительная	1
Низкая	2
Средняя	3

Важность тега	Вес тега
Высокая	4
Критическая	5

Пользователи с правами администратора могут управлять тегами в разделе **Параметры** веб-интерфейса Kaspersky CyberTrace или с помощью запросов REST API.

Работа с тегами индикатора

На странице **Индикаторы** можно управлять тегами индикатора путем назначения существующих тегов, добавления новых тегов или снятия тегов. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Работа с тегами индикатора выполняется в следующем порядке:

1. Нажмите на значение необходимого индикатора.
2. На открывшейся странице **Сведения об индикаторе** прокрутите вниз до раздела **Теги**.

Присвоение индикатору существующих тегов

Чтобы присвоить индикатору теги, выполните следующие действия:

1. Нажмите на кнопку **Назначить существующие теги**.
2. В списке тегов установите флажки для тегов, которые требуется назначить индикатору.

   В список входят только те теги, которые уже существуют в Kaspersky CyberTrace. Если требуется добавить новый тег, выполните действия в соответствии с инструкцией, приведенной ниже.
3. Нажмите на кнопку **Применить**.

Выбранные теги назначаются индикатору.

Добавление нового тега к индикатору

Для добавления тега необходимы права администратора.

Чтобы добавить новый тег к индикатору:

1. Нажмите на кнопку **Добавить тег**.
2. В открывшемся диалоговом окне **Добавить тег** выполните следующие действия:
   - Задайте имя тега. Длина тега должна составлять от 1 до 128 символов. Тег может содержать латинские буквы, цифры, дефисы (-) и знаки подчеркивания (_). Для нового тега нельзя использовать имя уже существующего тега.
   - Выберите важность тега.
   - Не снимайте флажок **Назначить тег индикатору**.

     Если снять этот флажок, тег будет создан, но не будет назначен выбранному индикатору.
3. Нажмите на кнопку **Добавить**.

   Новый тег будет создан и назначен индикатору.

Снятие тега с индикатора

Снятие тегов с индикаторов не приводит к удалению этих тегов из Kaspersky CyberTrace.

Чтобы снять назначенный тег с индикатора, выполните следующие действия:

1. Нажмите на кнопку (**Снять**) рядом с тегом, который требуется снять.
2. В открывшемся окне подтверждения нажмите кнопку **Снять**.

Выбранный тег снимается с индикатора.

Фильтрация индикаторов по тегам

При просмотре индикаторов можно фильтровать записи по тегам или по суммарному весу тегов. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Фильтрация индикаторов по тегам

Чтобы отфильтровать индикаторы по тегу, выполните следующие действия:

1. Нажмите на значок (воронка) в столбце **Теги** таблицы.
2. В открывшемся диалоговом окне установите флажки рядом с тегами, по которым необходимо отобрать отображаемые индикаторы. Можно выбрать несколько тегов одновременно.

В таблице отображаются выбранные записи.

Фильтрация индикаторов по суммарному весу тегов

У каждого тега есть вес от 0 до 5, в зависимости от важности тега. Если индикатору назначено несколько тегов, их веса суммируются.

Чтобы отфильтровать индикаторы по суммарному весу тегов, выполните следующие действия:

1. Нажмите на значок ▽ (воронка) в столбце **Общий вес тегов** таблицы.
2. В открывшемся диалоговом окне укажите минимальное и максимальное значения веса тегов.
3. Нажмите на кнопку **Применить**.

В таблице отображаются выбранные записи.

Просмотр задач

Чтобы быть в курсе текущего состояния и использования Kaspersky CyberTrace, в Kaspersky CyberTrace можно просматривать информацию о задачах. Для работы с этим разделом необходимо перейти в режим **Управление системой**. Этот режим доступен только пользователям с ролью «Администратор».

Информация о задачах отображается на странице **Задачи**.

В Kaspersky CyberTrace есть два типа задач:

- Задачи, запускаемые пользователем (задачи по требованию).
- Задачи, запускаемые Kaspersky CyberTrace (фоновые задачи по расписанию).

Предоставляется доступ ко всем задачам, запущенным всеми администраторами, а также к фоновым задачам по расписанию. Чтобы определить тип задачи, достаточно взглянуть на ее свойство **Название**: для фоновых задач по расписанию отображается **Система**.

Предоставляется доступ к информации о следующих фоновых задачах по расписанию:

- Регулярное обновление потоков данных об угрозах.
- Расчет пересечения источников данных об угрозах, используемых в Kaspersky CyberTrace.
- Регулярное ретроспективное сканирование.
- Регулярное обновление экспорта индикаторов.
- Создание и отправка отчетов на адреса электронной почты.
- Предварительно заданные параметры экспорта индикаторов.

Для каждой задачи в списке приводится следующая информация:

- Имя задачи.
- Статус задачи:
  - **Выполняется**

    Задача будет запущена.
  - **Выполнена**

    Задача успешно выполнена.

- **Выполнена (частично)**

  Этот статус относится к задачам обновления потоков данных. Задача считается частично выполненной, если хотя бы один индикатор обработанного потока даных не прошел валидацию Kaspersky CyberTrace.

- **Ошибка**

  Задача не выполнена из-за сбоя при обработке потоков данных.

- **Отменена**

  Задача отменена пользователем.

Путем выключения переключателя **Показывать системные задачи** можно отключить отображение состояния задач по расписанию.

Kaspersky CyberTrace проверяет добавляемые в систему индикаторы IP, HASH (MD5, SHA1 и SHA256) с помощью регулярных выражений.

Проверка индикаторов IP выполняется, если обнаруживается следующее:

- Четыре октета.
- Октеты разделены точками.
- Значение каждого октета попадает в диапазон от 0 до 255.
- Нет ведущих нулей.
- Допустимые символы: цифры, точка (".").

Проверка индикаторов хешей (MD5, SHA1, SHA256) выполняется, если обнаруживается следующее:

- Длина хеша составляет 32 символа для MD5, 40 символов для SHA1, 64 символа для SHA256.
- Допустимые символы: 0–9, a–f, A–F.
- Допускаются символы как в верхнем, так и в нижнем регистре.

Если хотя бы один индикатор не пройдет проверку во время обновления задачи, то при наведении курсора на значок статуса задачи появится всплывающая подсказка с текстом в следующем формате:

- Название потока данных, индикаторы которого не прошли проверку.
- Количество индикаторов потока данных, не прошедших проверку.
- Общее количество индикаторов потока данных.

- Имя пользователя, запустившего задачу, или **Система** для фоновых задач по расписанию.
- Дата и время запуска задачи.
- Дата и время завершения задачи.

Список можно отсортировать нажатием на заголовки столбцов.

Kaspersky CyberTrace обновляет список каждую секунду и хранит информацию о каждой задаче в течение семи дней.

Приложение для Splunk

В этой главе описывается порядок использования приложения Kaspersky CyberTrace App для Splunk.

О приложении Kaspersky CyberTrace App для Splunk

Kaspersky CyberTrace App для Splunk представляет собой приложение для Splunk. Его назначение заключается в следующем:

- Отображение информации об URL, IP-адресах и хешах событий, сопоставленных с потоками данных об угрозах Kaspersky Threat Data Feeds, на информационной панели **Kaspersky CyberTrace Matches**.
- Отображение информации о состоянии Kaspersky CyberTrace на информационной панели **Kaspersky CyberTrace Status**.
- Сопоставление отдельных URL, IP-адресов и хешей с потоками данных об угрозах Kaspersky Threat Data Feeds путем выполнения поиска на вкладке **Indicators lookup**.
- Выполнение самостоятельной диагностики и отображение используемых потоков данных об угрозах.

Кроме того, Kaspersky CyberTrace App для Splunk поставляется с шаблонами оповещений, демонстрирующими основные условия срабатывания, которые можно использовать с Kaspersky CyberTrace.

Об информационных панелях Kaspersky CyberTrace App

В Kaspersky CyberTrace App используются следующие информационные панели:

- **Kaspersky CyberTrace Matches**

  На этой информационной панели представлена информация об URL, IP-адресах и хешах событий, сопоставленных с потоками данных об угрозах Kaspersky Threat Data Feeds, а также статистическая информация и журнал совпадений.

- **Kaspersky CyberTrace Status**

  На этой информационной панели отображается статистика сопоставления для Kaspersky CyberTrace Service и журнал оповещений, полученных от Kaspersky CyberTrace Service. Также на этой информационной панели можно запустить самостоятельную диагностику Kaspersky CyberTrace App для Splunk.

- **Indicators lookup**

  На этой вкладке осуществляется настройка и выполнение поиска по индикатору.

- **Alerts**

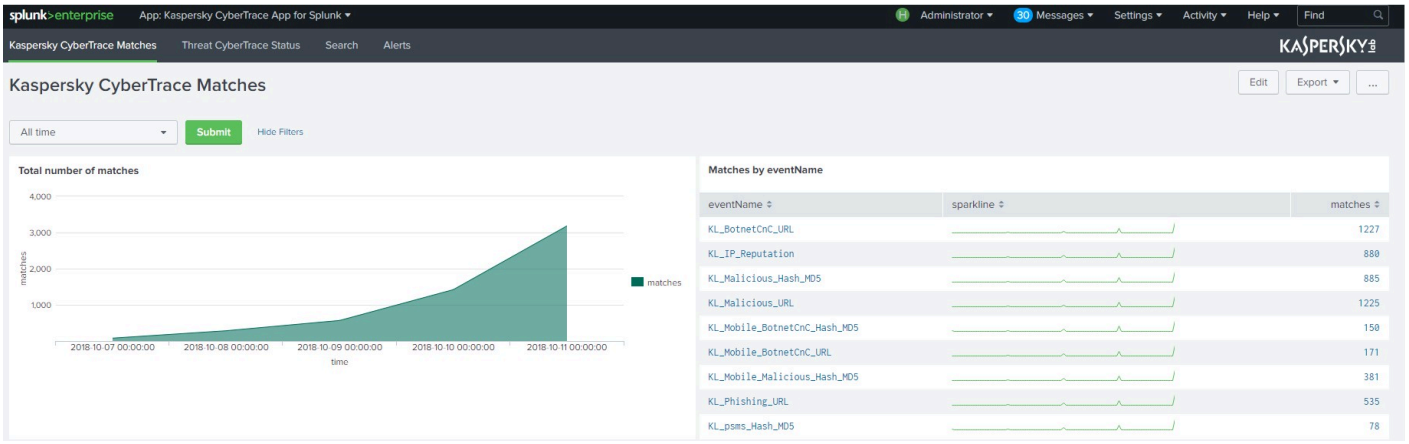
  Это стандартная информационная панель «Alerts». В Kaspersky CyberTrace App для Splunk входит несколько шаблонов оповещений, которые можно использовать и настраивать на этой информационной панели.

- **Kaspersky CyberTrace online documentation**

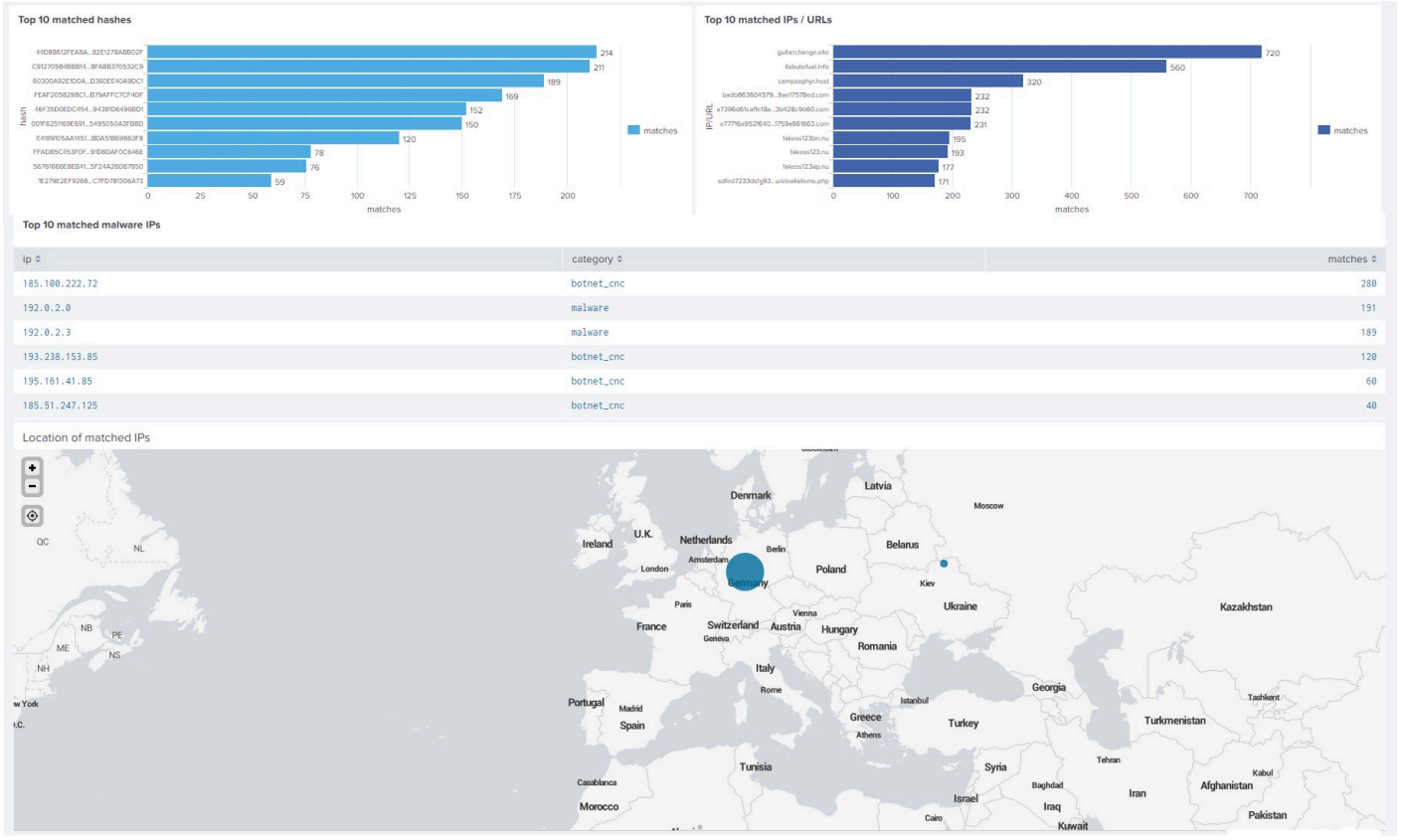
  Ссылка на онлайн-документацию Kaspersky CyberTrace.

Информационная панель Kaspersky CyberTrace Matches

На информационной панели **Kaspersky CyberTrace Matches** отображается информация о URL, IP-адресах и хешах из событий, сопоставленных с потоками данных об угрозах Kaspersky Threat Data Feeds, а также статистическая информацию и журнал сопоставления.



Информационная панель **Kaspersky CyberTrace Matches**



Панели **Top 10**



Панель **Match log**

На этой информационной панели предусмотрен инструмент выбора временного диапазона и несколько панелей:

- Инструмент выбора временного диапазона

  С его помощью можно выбрать временной диапазон для отображаемой информации.

- Total number of matches

  На этой панели отображается диаграмма суммарного количества обнаруженных киберугроз по всем потокам данных об угрозах, которые используются в Kaspersky CyberTrace Service.

- Matches by `eventName`

  На этой панели отображается таблица с количеством киберугроз для каждой категории.

- Top 10 matched hashes

  На этой панели отображается гистограмма 10 хешей, наиболее часто встречающихся среди обнаруженных киберугроз.

- Top 10 matched IPs / URLs

  На этой панели отображаются гистограммы 10 IP-адресов и URL, наиболее часто встречающихся среди обнаруженных киберугроз.

- Top 10 matched TOR / malware / spam IPs

  На этой панели отображается список из 10 вредоносных IP-адресов, IP-адресов выходных узлов Tor® и IP-адресов, связанных со спамом, наиболее часто встречающихся среди обнаруженных киберугроз.

- Location of matched IPs

  На этой панели отображается карта с местоположениями обнаруженных IP-адресов.

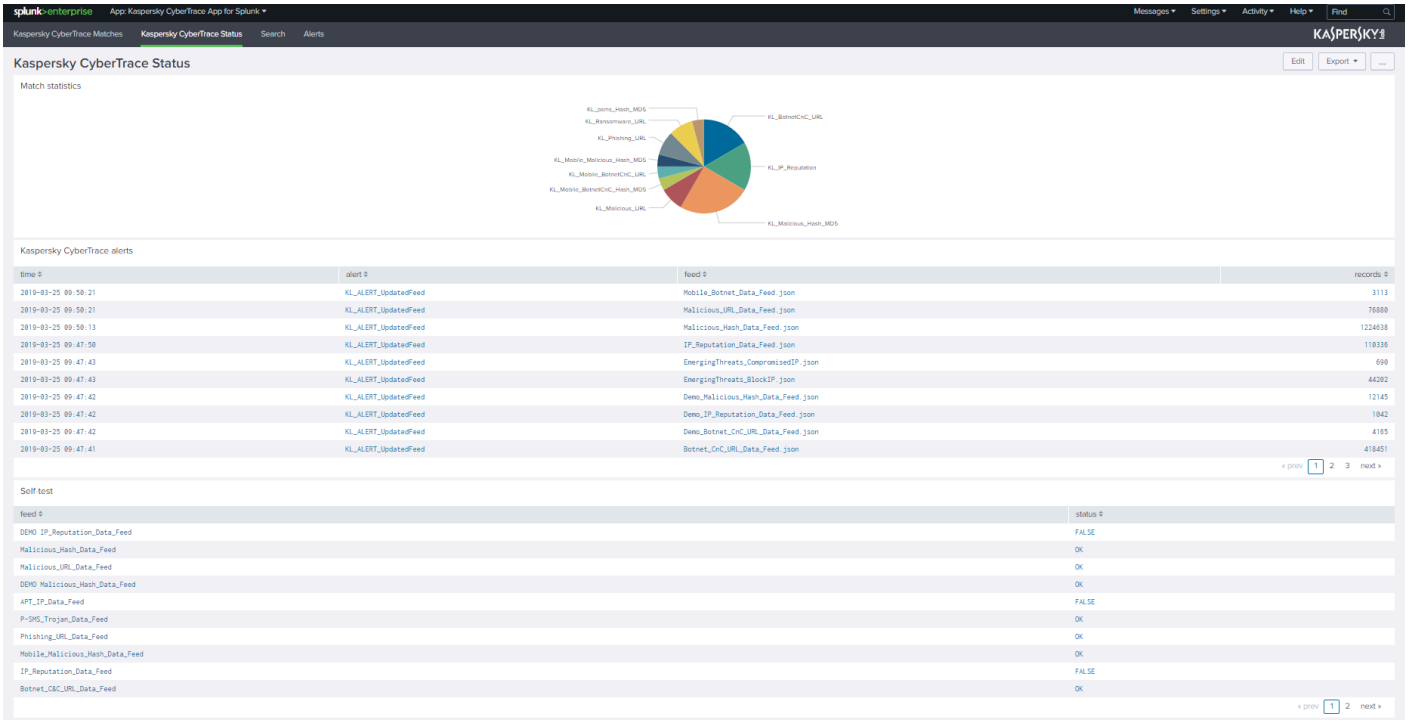
- Match log

На этой панели отображается таблица с журналом всех обнаруженных киберугроз, включая контекстную информацию о каждой киберугрозе. Отображаются поля контекста, перечисленные ниже. Это поля, которые можно добавлять в исходящие события отдельно от общего контекста записей потока данных об угрозах.

- First_seen
- Last_seen
- Popularity
- Threat
- Publication name
- Industry
- Threat_score
- File_size
- Behavior

Информационная панель Kaspersky CyberTrace Status

На информационной панели **Kaspersky CyberTrace Status** предоставляется статистика обнаруженных киберугроз для Feed Service и отображается журнал оповещений, которые были сгенерированы Kaspersky CyberTrace Service.



Информационная панель **Kaspersky CyberTrace Status**

Информационная панель **Kaspersky CyberTrace Status** состоит из трех панелей:

- Панель **Match statistics**
- Панель **Kaspersky CyberTrace alerts**
- Панель **Self test**

Панель «Match statistics»

На этой панели отображается круговая диаграмма обнаруженных киберугроз по каждой категории, возвращаемой Kaspersky CyberTrace Service.

Панель «Kaspersky CyberTrace alerts»

На этой панели отображается таблица с журналом оповещений, сгенерированных Kaspersky CyberTrace Service.

Панель «Self test»

На этой панели отображается таблица с результатами самостоятельной диагностики

Данные настройки используются для выполнения самостоятельной диагностики на вкладке «Kaspersky CyberTrace Status».

Самостоятельная диагностика выполняется автоматически при открытии информационной панели **Kaspersky CyberTrace Status**. Возможны следующие значения статуса:

- OK

  Поток данных об угрозах включен, и сопоставление для этого потока данных об угрозах прошло успешно.

- FALSE

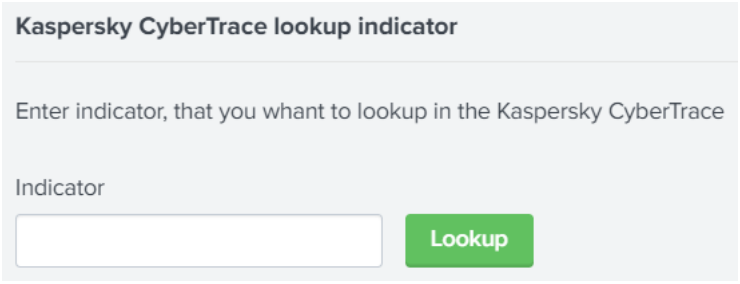
  Поток данных об угрозах отключен или Feed Utility или Kaspersky CyberTrace Service неправильно его обрабатывают.

Для поиска используются настройки подключения Kaspersky CyberTrace. Данные параметры задаются на вкладке **Indicators lookup**.

Indicators lookup

На вкладке **Indicators lookup** можно выполнять следующие действия:

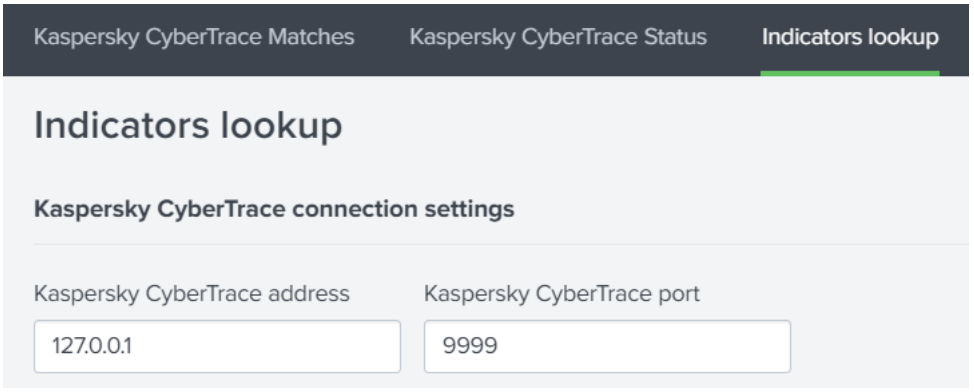
- Выполнять поиск по отдельному индикатору. Можно использовать следующие форматы:
  - `%INDICATOR%`, если Kaspersky CyberTrace использует общие регулярные выражения (регулярные выражения, не привязанные к конкретному полю).
  - `%FIELDNAME%=%INDICATOR%`, если Kaspersky CyberTrace использует регулярные выражения, ожидающие, что значение `%INDICATOR%` будет указано в поле `%FIELDNAME%`.



Поиск по одному индикатору

- Чтобы настроить поиск по индикатору, выполните следующие действия: Эти настройки будут применены к любому индикатору, задействованному в процессе поиска, только в том случае, если поиск выполняется по какому-либо индикатору. Эти настройки также используются для выполнения самостоятельной диагностики на вкладке **Kaspersky CyberTrace Status**. Настройки будут помещены в хранилище Splunk.

  В этом разделе можно указать IP-адрес и порт Kaspersky CyberTrace.



Настройки подключения Kaspersky CyberTrace

- Чтобы просмотреть подробную информацию об индикаторе, выполните следующие действия:

  Чтобы подробнее изучить необходимый индикатор, нажмите на результат поиска. Ссылка ведет на страницу Kaspersky Threat Intelligence Portal, на которой приведена информация об объекте.

Шаблоны информационных сообщений

Kaspersky CyberTrace App для Splunk поставляется с несколькими шаблонами оповещений, которые можно использовать и настраивать на информационной панели **Alerts**.

Шаблоны и триггеры оповещений

Доступны следующие шаблоны оповещений:

- Информационное сообщение «Matches»

  Это оповещение срабатывает, если за последние 24 часа были обнаружены киберугрозы при сопоставлении с потоками данных об угрозах Kaspersky Threat Data Feeds.

- Информационное сообщение «No Matches»

  Это оповещение срабатывает, если за последние 24 часа не было обнаружено киберугроз при сопоставлении с потоками данных об угрозах Kaspersky Threat Data Feeds.

- Информационное сообщение «Emergency»

  Это оповещение срабатывает, если в течение одной минуты было обнаружено 5000 киберугроз по потокам данных об угрозах Kaspersky Threat Data Feeds.

- Оповещение «Service Unavailable»

  Это оповещение срабатывает в случае недоступности Kaspersky CyberTrace Service.

  Это оповещение содержит дату создания оповещения, за которой следует отметка времени в формате UNIX time.

- Оповещение «Service Started»

  Это оповещение срабатывает при запуске Kaspersky CyberTrace Service.

  Это оповещение содержит дату создания оповещения, за которой следует отметка времени в формате UNIX time.

Действия с оповещениями

По умолчанию действие `Add to Triggered Alerts` определено для всех оповещений. В качестве варианта можно добавить действие «Send email», чтобы Splunk отправлял электронное сообщение на адрес электронной почты, указанный для этого действия.

Создание уведомлений о входящих служебных событиях

Для создания уведомлений о входящих служебных событиях Kaspersky CyberTrace можно настроить правила оповещений.

Чтобы создать уведомления о служебных событиях из Kaspersky CyberTrace в Splunk, выполните следующие действия:

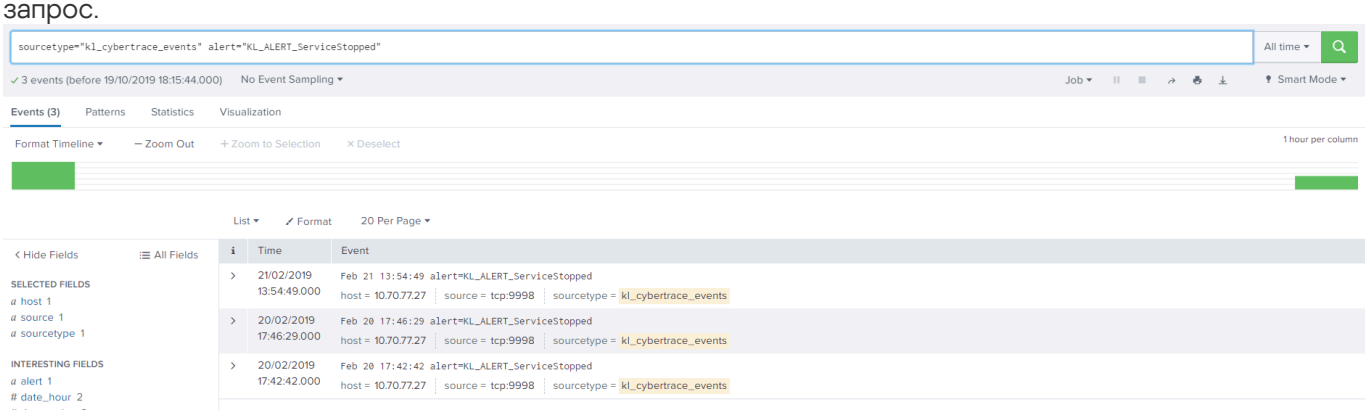
1. В меню **Search and Reporting app for Splunk** выберите вкладку **Search**.

2. В поле поиска укажите условие для создания оповещений. Например:

   ```
   sourcetype="kl_cybertrace_events" alert="KL_ALERT_ServiceStopped"
   ```

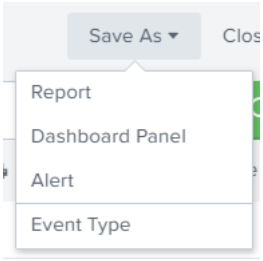
   Это условие определяет запрос на поиск оповещений о событиях, которые генерируются при остановке Kaspersky CyberTrace Service.

3. Нажмите на кнопку «Search» ( ), чтобы проверить, правильно ли выполняется сформулированный запрос.



KL_ALERT_ServiceStopped events

4. Нажмите на кнопку **Save as** и выберите **Alert**.



Сохранение оповещения

Откроется окно **Save As Alert**.

5. В окне **Save As Alert** задайте следующие настройки:

- В поле **Title** укажите имя оповещения.

  Указываемое название может быть любым.

- В поле **Description** укажите описание оповещения.

  Указываемое описание может быть любым.

- В поле **Alert type** выберите один из следующих вариантов:

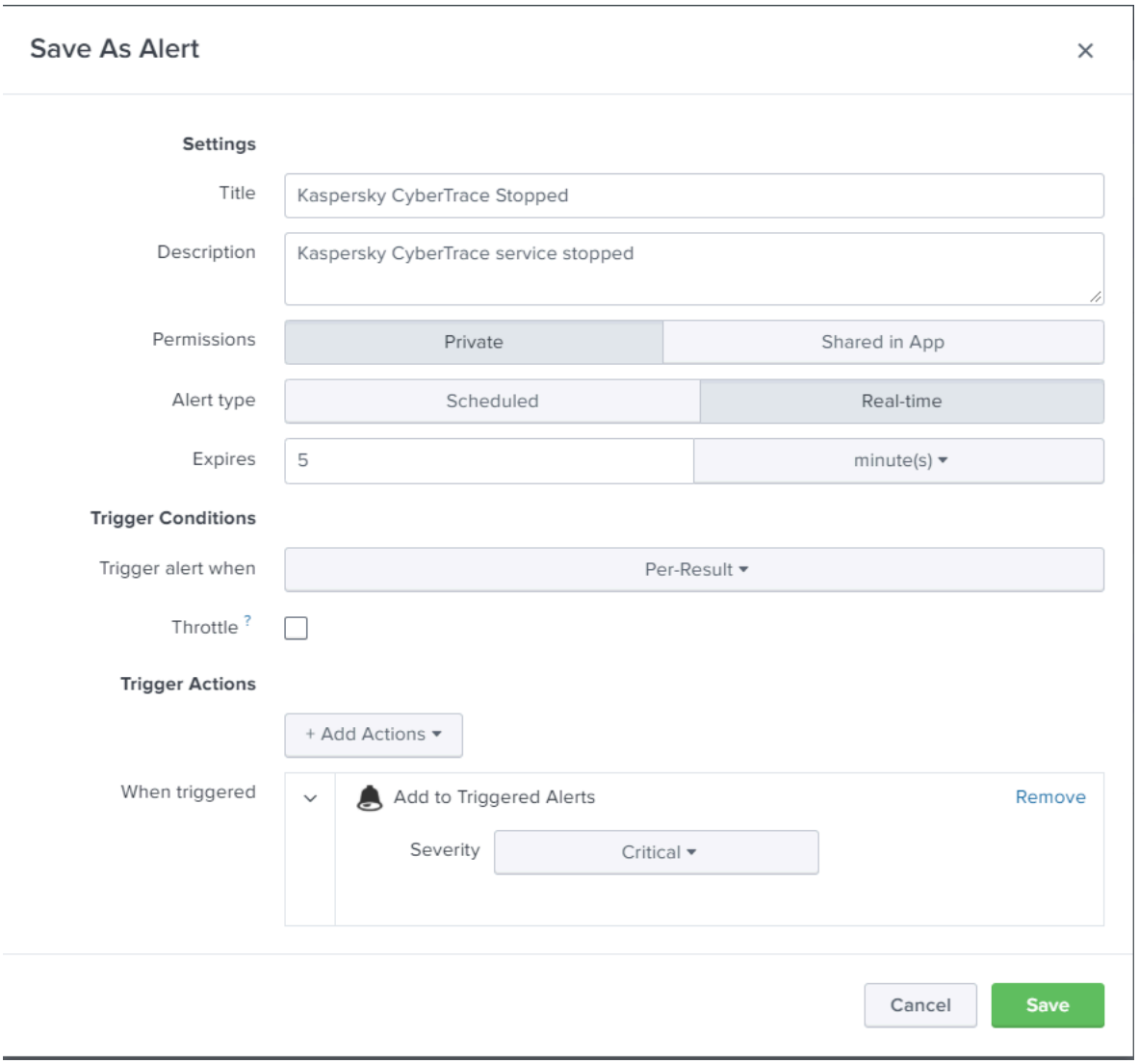
  - **Scheduled**, если требуется регулярно проверять события на соответствие указанным условиям.

  - **Real-time**, если требуется проверять события на соответствие указанным условиям в режиме реального времени.

- В поле **Trigger** укажите **For each results**.

- Установите флажок **Throttle**, а затем, если необходимо, укажите продолжительность интервала времени, в течение которого Splunk не будет отправлять новые оповещения в случае срабатывания правила.

- В поле **Trigger Actions** укажите способ, которым Splunk будет уведомлять о срабатывании оповещения.



Окно **Save As Alert**

6. Нажмите на кнопку **Save**.

   Правило появится в Splunk.

Работа с событиями в ArcSight

В этой главе описывается порядок работы с событиями в ArcSight.

Информационные панели

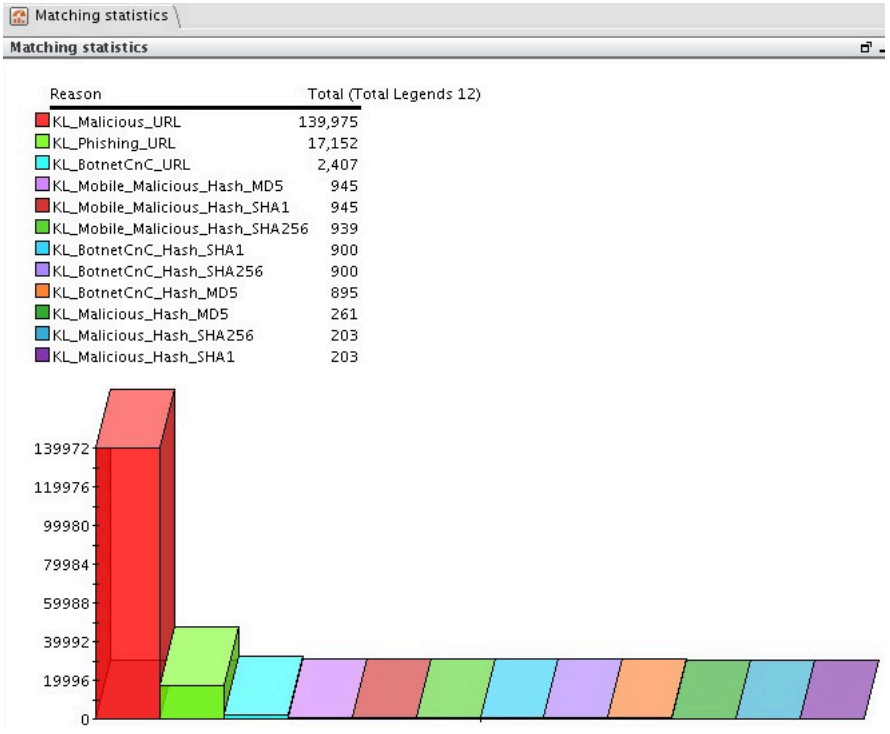
После импорта пакета ARB в ArcSight становятся доступны следующие информационные панели:

- **CyberTrace Detection map**

  Отображаются все устройства, которые отправляли события, содержащие вредоносные URL, IP-адреса или хеши. На карте отображаются все потоки данных об угрозах, задействованные в процессе обнаружения киберугроз.

- **CyberTrace match statistics**

  Статистика обнаружений киберугроз: сколько раз определенный поток данных об угрозах был задействован в процессе обнаружения. Если поток данных об угрозах не был задействован в процессе обнаружения киберугроз, он не отображается на информационной панели.



Информационная панель **Matching statistics**

- **CyberTrace TOP 10 matched indicators**

  Содержит три диаграммы:

  - CyberTrace TOP 10 matched IPs

    Топ-10 обнаруженных IP-адресов.

  - CyberTrace TOP 10 matched URLs

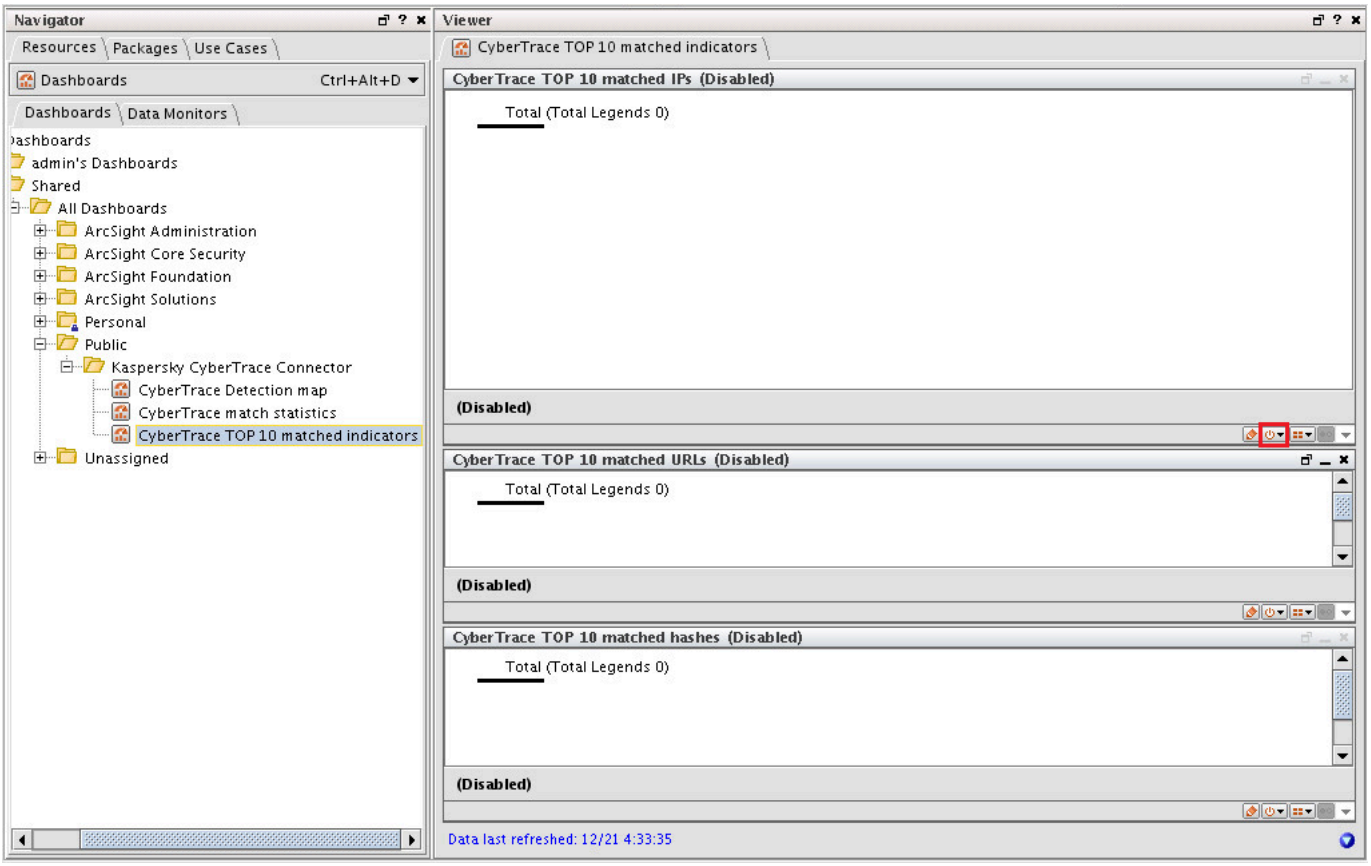
    Топ-10 обнаруженных URL.

  - CyberTrace TOP 10 matched hashes

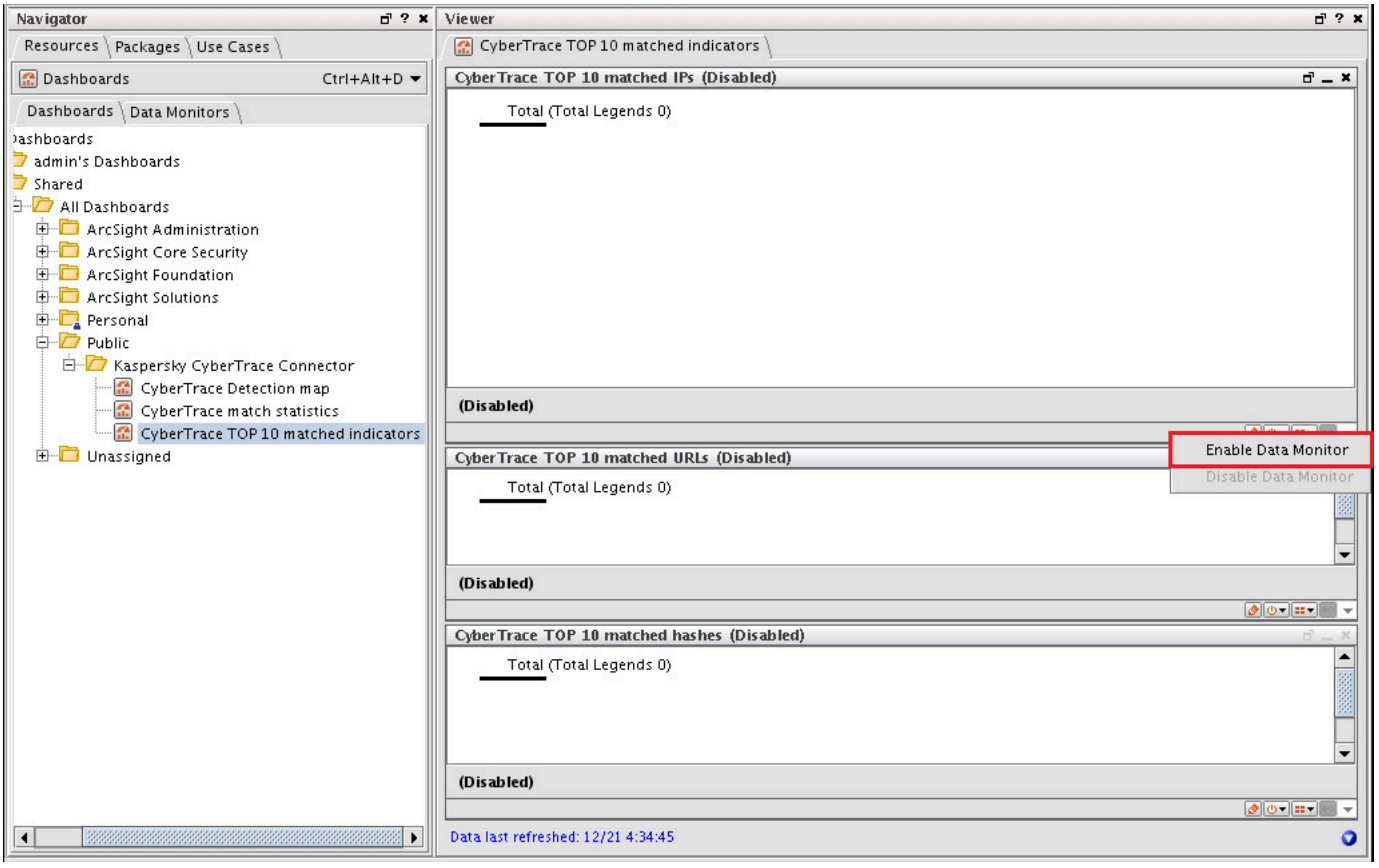
    Топ-10 обнаруженных хешей.

На информационных панелях отображаются данные, полученные за последние 48 часов.

Чтобы включить отключенную информационную панель, необходимо нажать на кнопку **Enable Data Monitor** ( ) и в раскрывающемся списке выбрать **Enable Data Monitor**.

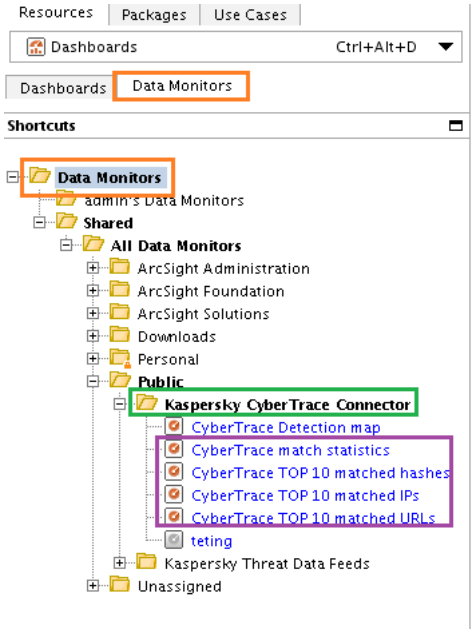


Кнопка **Enable Data Monitor**



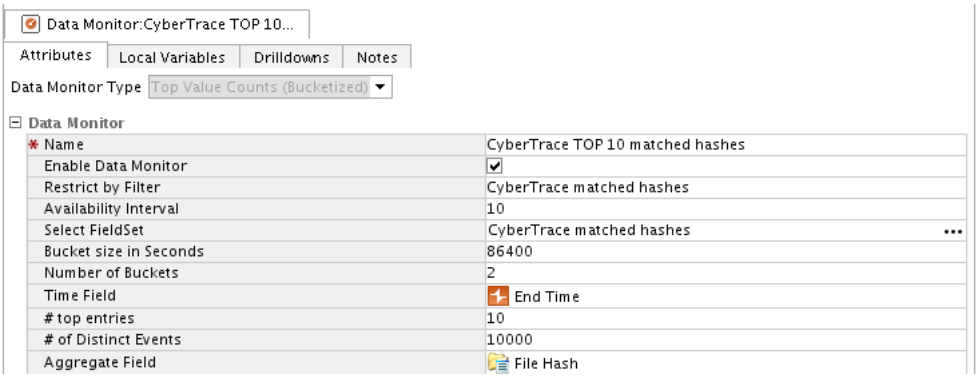
Включение информационной панели в версиях 6.8 и 6.11

Приведенные выше инструкции относятся к ArcSight ESM версий 6.8 и 6.11. Чтобы начать использовать информационную панель в ArcSight ESM версии 7.0, выберите **Dashboards,** затем вкладку **Data Monitors**. В дереве консоли выберите **Data Monitors** → **Shared** → **All Data Monitors** → **Public**.



Включение информационной панели в ArcSight ESM версии 7.0

Щелкните правой кнопкой мыши **Kaspersky CyberTrace Connector** и выберите пункт **Edit Data Monitor**. На вкладке **Attributes** укажите `300` в качестве значения параметра **Bucket size in Seconds** и `288` в качестве значения параметра **Number of Buckets**.



Редактирование Data Monitor

После выполнения этих действий на информационной панели отображаются данные за последние 24 часа. Выполните те же действия для всех мониторов, кроме **CyberTrace Detection map**.

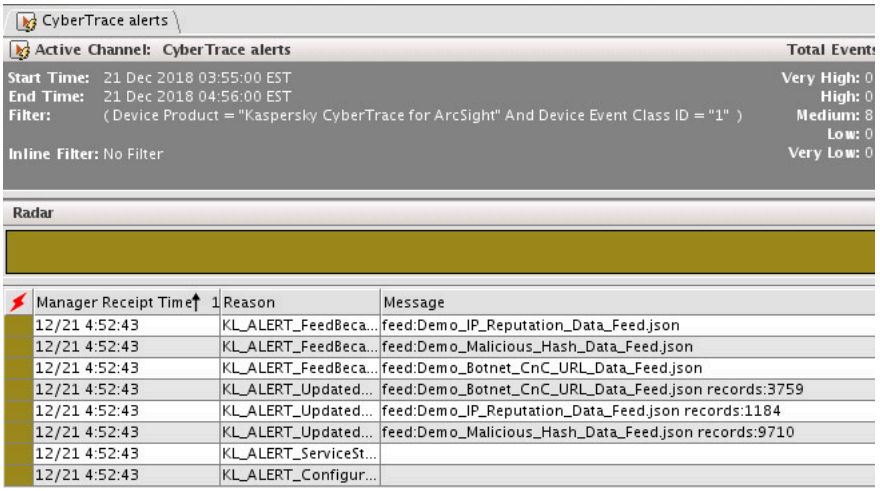
Активные каналы

После импорта пакета ARB в ArcSight становятся доступны следующие активные каналы:

- **CyberTrace alerts**

Отображает служебные оповещения из службы Kaspersky CyberTrace в режиме реального времени.

- Поле **Reason** содержит идентификатор служебного оповещения.
- Поле **Message** содержит дополнительную информацию об оповещении (если есть).



Активный канал **CyberTrace alerts**

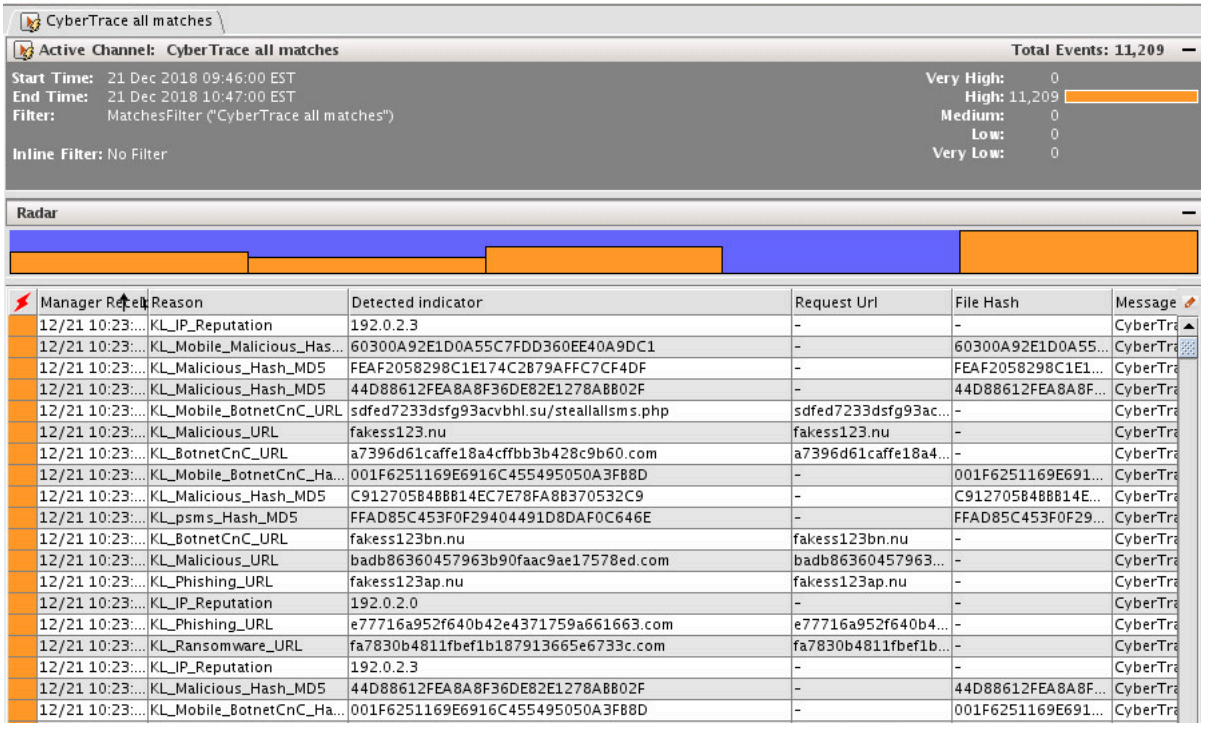
- **CyberTrace all matches**

  Отображает оповещения об обнаружении индикаторов компрометации из службы Kaspersky CyberTrace в режиме реального времени.

  - В поле **Reason** указывается категория обнаруженного объекта.
  - Поле **Detected indicator** содержит обнаруженный объект.
  - В поле **Request Url** содержится URL, который был обнаружен в событии, отправленном из ArcSight в Kaspersky CyberTrace Service.
  - В поле **File Hash** содержится хеш, который был обнаружен в событии, отправленном из ArcSight в Kaspersky CyberTrace Service.
  - В поле **Source Service Name** содержится название производителя устройства, отправившего событие в ArcSight.
  - В поле **Source Process Name** содержится имя устройства, отправившего событие в ArcSight.
  - В поле **Event Outcome** содержится идентификатор исходного события, которое поступило в ArcSight и затем было отправлено в Kaspersky CyberTrace Service.
  - В поле **Message** содержится краткое описание обнаружения киберугрозы. Описание имеет следующий формат: `CyberTrace detected <имя_потока_данных_об_угрозах_задействованного_в_процессе_обнаружения_киберугроз>`.
  - В поле **Source User Name** содержится имя пользователя, который был активен на о конечном устройстве.
  - В поле **Source Address** содержится IPv4-адрес, идентифицирующий источник, на который ссылается исходное событие.
  - В поле **Destination Address** содержится IPv4-адрес назначения, который был обнаружен в событии, отправленном из ArcSight в Kaspersky CyberTrace Service.

- В поле **Device Action** содержится действие, выполненное устройством, как указано в исходном событии.

- Значения полей **Popularity**, **Threat Score**, **Threat** и других берутся из потока данных об угрозах, который был задействован в процессе обнаружения киберугроз.



Manager Receipt	Reason	Detected indicator	Request Url	File Hash	Message
12/21 10:23:...	KL_IP_Reputation	192.0.2.3	-	-	CyberTra
12/21 10:23:...	KL_Mobile_Malicious_Has...	60300A92E1D0A55C7FDD360EE40A9DC1	-	60300A92E1D0A55...	CyberTra
12/21 10:23:...	KL_Malicious_Hash_MD5	FEAF2058298C1E174C2B79AFFC7CF4DF	-	FEAF2058298C1E1...	CyberTra
12/21 10:23:...	KL_Malicious_Hash_MD5	44D88612FEA8A8F36DE82E1278ABB02F	-	44D88612FEA8A8F...	CyberTra
12/21 10:23:...	KL_Mobile_BotnetCnC_URL	sdfed7233dsfg93acvbhl.su/steallallsms.php	sdfed7233dsfg93ac...	-	CyberTra
12/21 10:23:...	KL_Malicious_URL	fakess123.nu	fakess123.nu	-	CyberTra
12/21 10:23:...	KL_BotnetCnC_URL	a7396d61caffe18a4cffbb3b428c9b60.com	a7396d61caffe18a4...	-	CyberTra
12/21 10:23:...	KL_Mobile_BotnetCnC_Ha...	001F6251169E6916C455495050A3FB8D	-	001F6251169E691...	CyberTra
12/21 10:23:...	KL_Malicious_Hash_MD5	C91270584BBB14EC7E78FA8B370532C9	-	C91270584BBB14E...	CyberTra
12/21 10:23:...	KL_psms_Hash_MD5	FFAD85C453F0F29404491D8DAF0C646E	-	FFAD85C453F0F29...	CyberTra
12/21 10:23:...	KL_BotnetCnC_URL	fakess123bn.nu	fakess123bn.nu	-	CyberTra
12/21 10:23:...	KL_Malicious_URL	badb86360457963b90faac9ae17578ed.com	badb86360457963...	-	CyberTra
12/21 10:23:...	KL_Phishing_URL	fakess123ap.nu	fakess123ap.nu	-	CyberTra
12/21 10:23:...	KL_IP_Reputation	192.0.2.0	-	-	CyberTra
12/21 10:23:...	KL_Phishing_URL	e77716a952f640b42e4371759a661663.com	e77716a952f640b4...	-	CyberTra
12/21 10:23:...	KL_Ransomware_URL	fa7830b4811fbef1b187913665e6733c.com	fa7830b4811fbef1b...	-	CyberTra
12/21 10:23:...	KL_IP_Reputation	192.0.2.3	-	-	CyberTra
12/21 10:23:...	KL_Malicious_Hash_MD5	44D88612FEA8A8F36DE82E1278ABB02F	-	44D88612FEA8A8F...	CyberTra
12/21 10:23:...	KL_Mobile_BotnetCnC_Ha...	001F6251169E6916C455495050A3FB8D	-	001F6251169E691...	CyberTra

Активный канал **CyberTrace all matches**

- **CyberTrace hash matches**

  Отображает оповещения об обнаружении хешей из службы Kaspersky CyberTrace в режиме реального времени.

- **CyberTrace URL matches**

  Отображает оповещения об обнаружении URL из службы Kaspersky CyberTrace в режиме реального времени.

- **CyberTrace IP matches**

  Отображает оповещения об обнаружении IP-адресов из службы Kaspersky CyberTrace в режиме реального времени.

Фильтрация событий для пересылки из ArcSight

В этом разделе описывается, как ArcSight фильтрует события, пересылаемые в Kaspersky CyberTrace Service.

Фильтр, импортированный из пакета ARB

После импорта пакета ARB ArcSight содержит фильтр `CyberTrace forwarding events`, используемый для фильтрации событий, которые будут пересылаться в Kaspersky CyberTrace Service.

Исходный фильтр `CyberTrace forwarding events` выбирает те события, которые содержат IP-адрес в поле `Destination Address`, URL в поле `Request URL` или хеш в поле `fileHash`, отправляемые устройством одного из следующих производителей:

- Cisco
- Microsoft®
- Juniper Networks™
- Trend Micro™
- McAfee®
- Imperva
- Check Point
- Blue Coat™
- Apache
- Fortinet
- Sourcefire®
- F5 Networks®
- FireEye™
- Palo Alto Networks
- Squid
- CyberTrace Verification Kit (для проверки работоспособности)

Кроме того, события, попадающие в выборку, формируемую исходным фильтром `CyberTrace forwarding events`, должны соответствовать одному из следующих условий:

- Поле `Source Address` или `Source Host Name` события не пустое, а значение поля `Destination Address` — не подсети `192.168.0.0/16`, `172.16.0.0/12` или `10.0.0.0/8`.
- Поле `Destination Address` или `Destination Host Name` события не пустое, а значение поля `Source Address` — не подсети `192.168.0.0/16`, `172.16.0.0/12` или `10.0.0.0/8`.
- Поле `Request URL` события содержит URL.
- Поле `fileHash` события содержит хеш.

Использование исходного фильтра `CyberTrace forwarding events` может значительно снизить производительность ArcSight ESM. Чтобы снизить нагрузку на сервер ArcSight ESM, отредактируйте фильтр так, чтобы он отправлял меньше событий или выполнял меньше проверок. Например, можно удалить из фильтра тех производителей, чьи события не поступают в ArcSight, или которые не нуждаются в проверке со стороны Kaspersky CyberTrace Service.

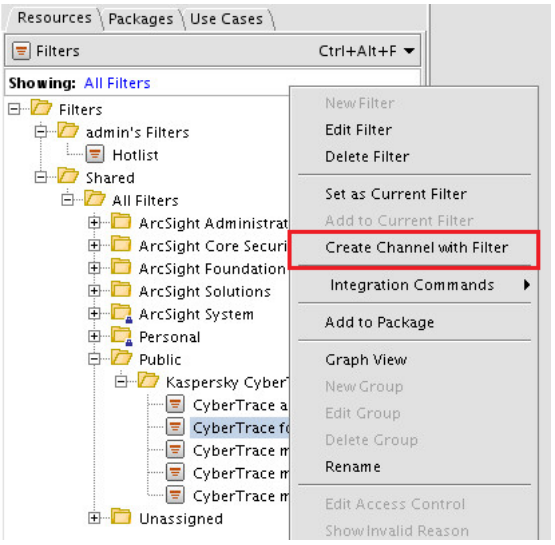
Проверка существующего фильтра

Может потребоваться проверить, попадают ли определенные события в выборку для существующего фильтра.

Чтобы проверить, попадают ли требуемые события в выборку, формируемую существующим фильтром, выполните следующие действия:

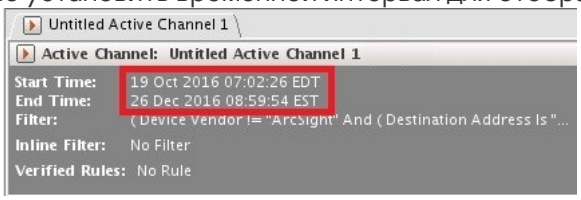
1. Создайте активный канал с фильтром.

   Щелкните правой кнопкой мыши по узлу фильтра в дереве **Filters** и выберите пункт контекстного меню **Create Channel with Filter**.



Создание канала

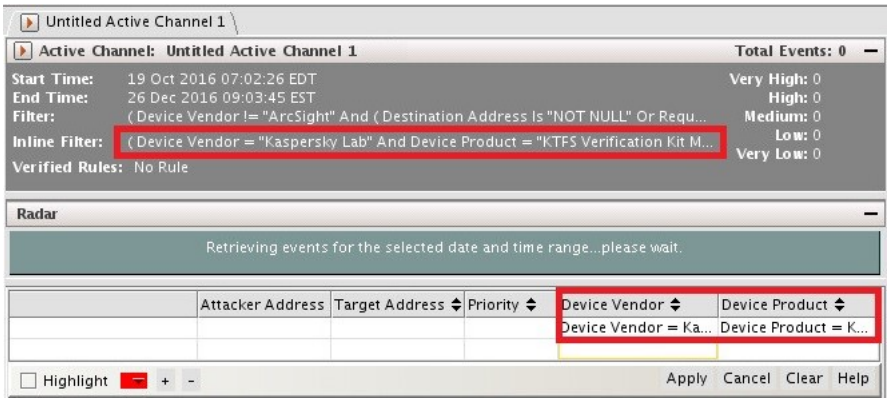
2. В случае необходимости можно установить временной интервал для отображения событий.



Настройка временного интервала

3. Если необходимо, в поле **Inline Filter** установите дополнительный фильтр, чтобы сузить выборку.

Например, можно задать для отображаемых событий производителя устройства, наименование изделия или и то, и другое.



Настройка дополнительного фильтра

4. Убедитесь, что события, которые требуется выбрать (и которые соответствуют добавленному условию), отображаются в созданном активном канале.

Изменение существующего фильтра

Существующий фильтр может потребоваться изменить. Например, если в активном канале не отображаются события от определенного производителя устройства, можно добавить производителя устройства в условие в фильтре, которое выполняет фильтрацию по производителям устройств.

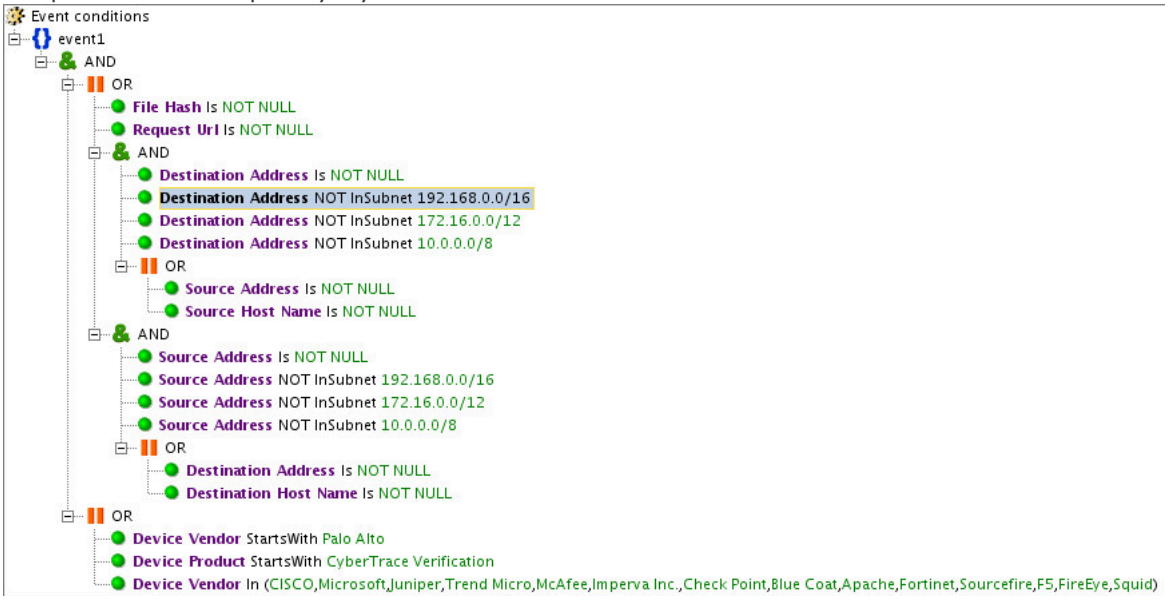
Чтобы добавить производителя устройства в фильтр, выполните следующие действия:

1. Откройте фильтр.

2. Выберите вкладку **Filter**.

   Отобразятся условия фильтрации, вложенные в элемент дерева **Event conditions**.

3. Измените условие **Device Vendor** и добавьте к нему производителя устройства, события которого должны отправляться в Kaspersky CyberTrace Service.



Условия фильтрации

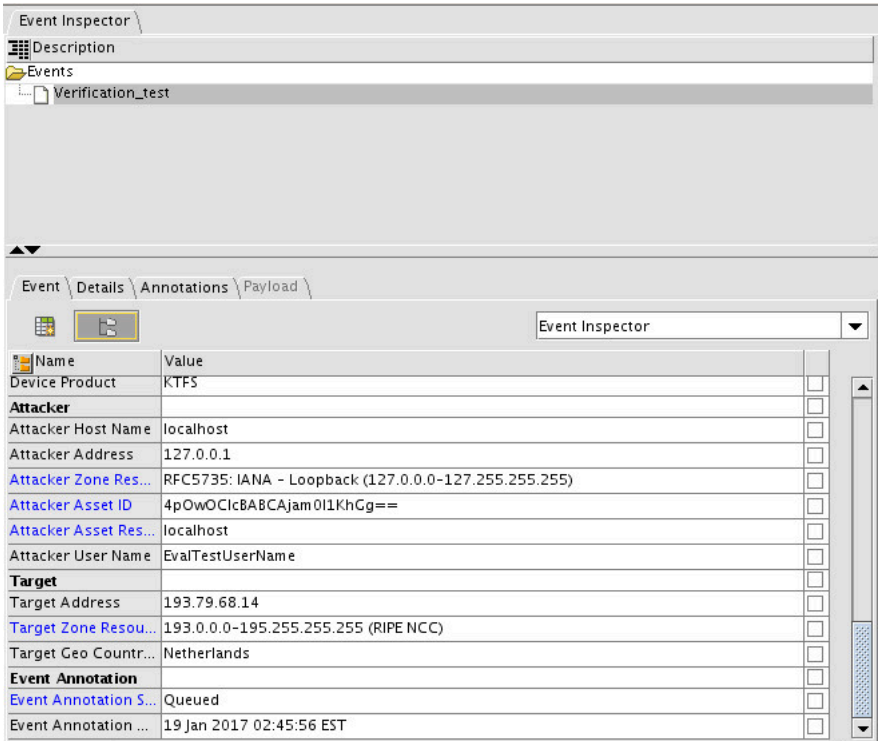
Просмотр информации о событиях в ArcSight

Информацию, содержащуюся в событии, можно просматривать, чтобы выбрать поля для фильтрации или для добавления к выходным событиям.

Чтобы просмотреть информацию о событиях в ArcSight,

в активном канале дважды щелкните событие, которое будет переслано в Kaspersky CyberTrace Service.

В ArcSight Console откроется вкладка **Event Inspector**, содержащая данные о событии.



Вкладка «Event Inspector»

Обратите внимание, что ArcSight и Kaspersky CyberTrace Service оперируют событиями в формате CEF, однако в ArcSight Console имена полей событий отображаются в удобочитаемой форме. В таблице ниже показано соответствие между некоторыми именами полей в этих двух представлениях.

Имена полей в формате CEF и в ArcSight Console

Имя поля в CEF	Имя поля в ArcSight Console
dst	Destination Address
dvc	Device Address
msg	Message
shost	Source Host Name

Создание уведомлений о входящих служебных событиях

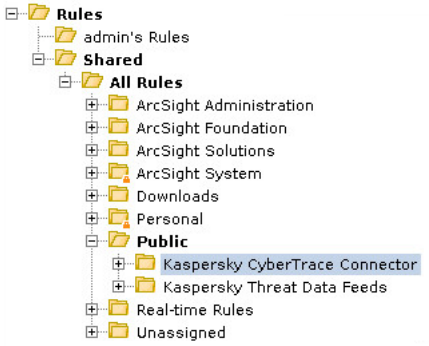
Для создания уведомлений о входящих служебных событиях Kaspersky CyberTrace можно настроить правила информационных сообщений.

Чтобы создать уведомления о служебных событиях из Kaspersky CyberTrace в ArcSight ESM, выполните следующие действия:

1. Запустите ArcSight Console.

2. На панели **Navigator** в раскрывающемся списке выберите **Rules**.

3. В дереве выберите **Rules** → **Shared** → **All Rules** → **Public directory**.



Дерево **Rules**

4. Щелкните правой кнопкой мыши узел фильтра в дереве **Kaspersky CyberTrace Connector** и выберите **New Rule** → **Standard Rule**.

5. На панели **Inspect** → **Edit** задайте следующие настройки:

   - В поле **Name** на вкладке **Attributes** укажите имя правила.

     Указываемое имя может быть любым.

- На вкладке **Conditions** укажите следующие условия:
  - `Device Product = Kaspersky CyberTrace for ArcSight`
  - `Reason = %ServiceEventCode%`

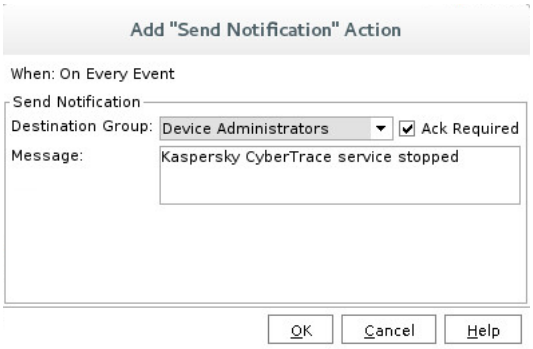
    Где `%ServiceEventCode%` — код [служебного события], который используется для генерации уведомлений.



Условия событий

- Щелкните правой кнопкой мыши вкладку **Actions**, выберите **On Every Event**, затем выберите следующее:
  - **Activate Trigger**
  - **Add**

    Эта настройка должна содержать действие, которое будет выполняться при получении служебного события, указанного на вкладке **Conditions**. Например, **Send Notification**.



Добавление действий

6. Нажмите на кнопку **Apply**.

Работа с событиями в RSA NetWitness

В этом разделе описывается порядок работы с событиями службы Kaspersky CyberTrace в RSA NetWitness.

Просмотр событий Kaspersky CyberTrace Service

В этом разделе описывается порядок просмотра в RSA NetWitness событий, поступающих из Kaspersky CyberTrace Service.

Чтобы отобразить в RSA NetWitness события, поступающие из Kaspersky CyberTrace Service, выполните следующие действия:

1. Убедитесь, что в RSA NetWitness включен экран **Navigate**.

По умолчанию в RSA NetWitness версии 11.6 и более поздних экран **Navigate** отключен. Чтобы включить экран **Navigate**, выполните следующие действия:

a. Перейдите в раздел (**Admin**) → **System** → **Investigation** → **Navigate**.

В версии 11.6.0 перейдите в раздел (**Admin**) → **System** → **Investigation** → **Investigate**.

b. Установите флажок **Enable Navigate**.

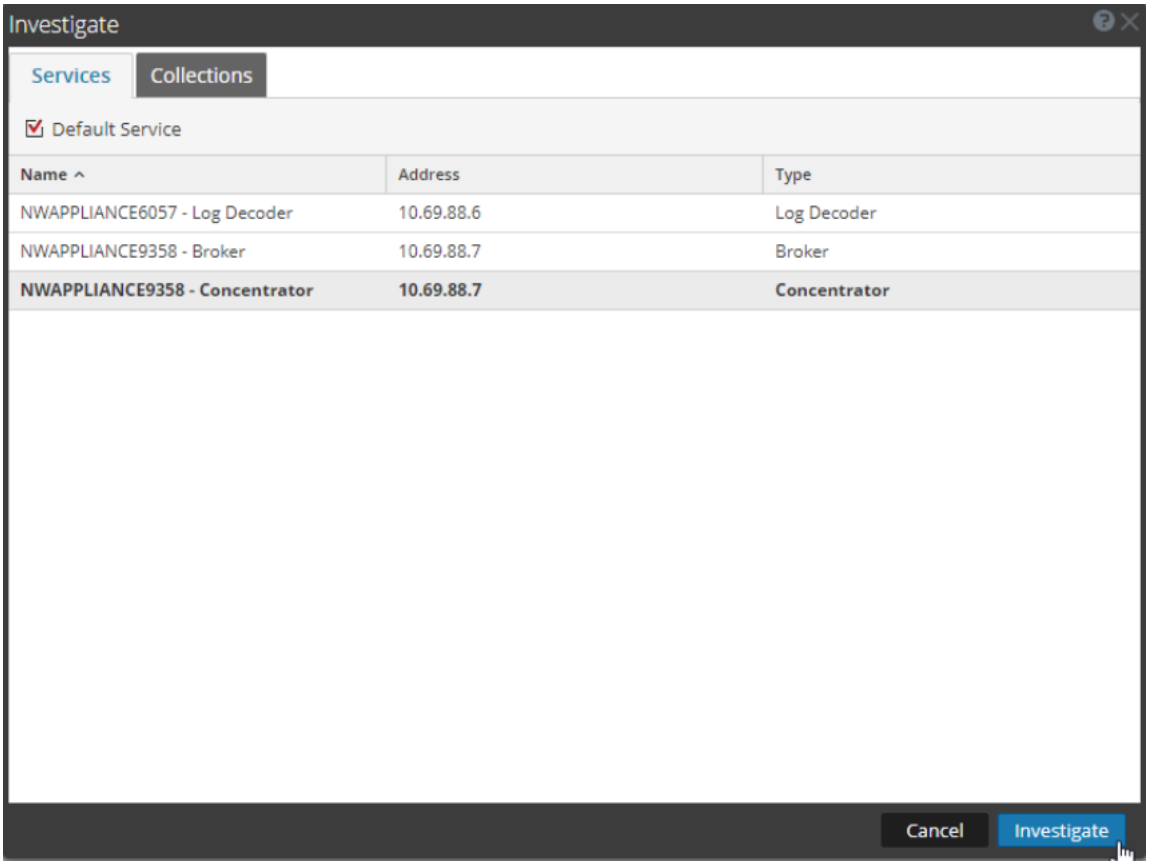
c. Нажмите на кнопку **Apply**.

2. В меню RSA NetWitness выберите **Investigation** → **Navigate**.

В версии 11.6.0 выберите **Investigate** → **Navigate**.

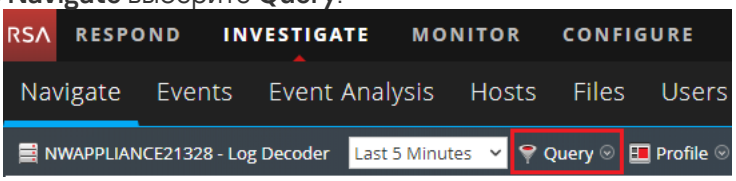
Откроется окно **Investigate**.

3. На вкладке **Services** выберите Concentrator, в котором хранятся события из Kaspersky CyberTrace Service (или Log Decoder, в который Kaspersky CyberTrace Service отправляет события), и нажмите кнопку **Investigate**.



Окно **Investigate**

4. На панели инструментов **Navigate** выберите **Query**.

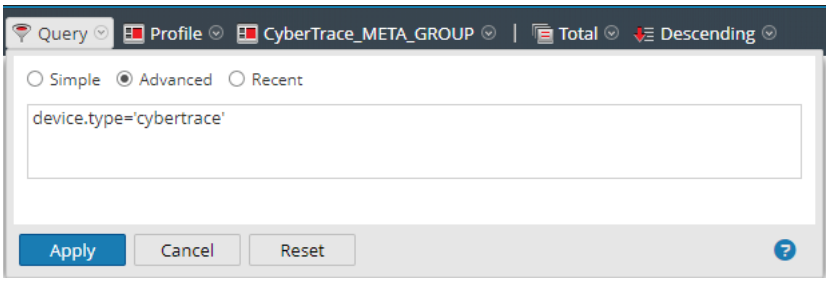


Кнопка панели инструментов **Query**

Откроется окно создания запроса (окно **Create**).

5. Выберите **Advanced** и введите следующий запрос:

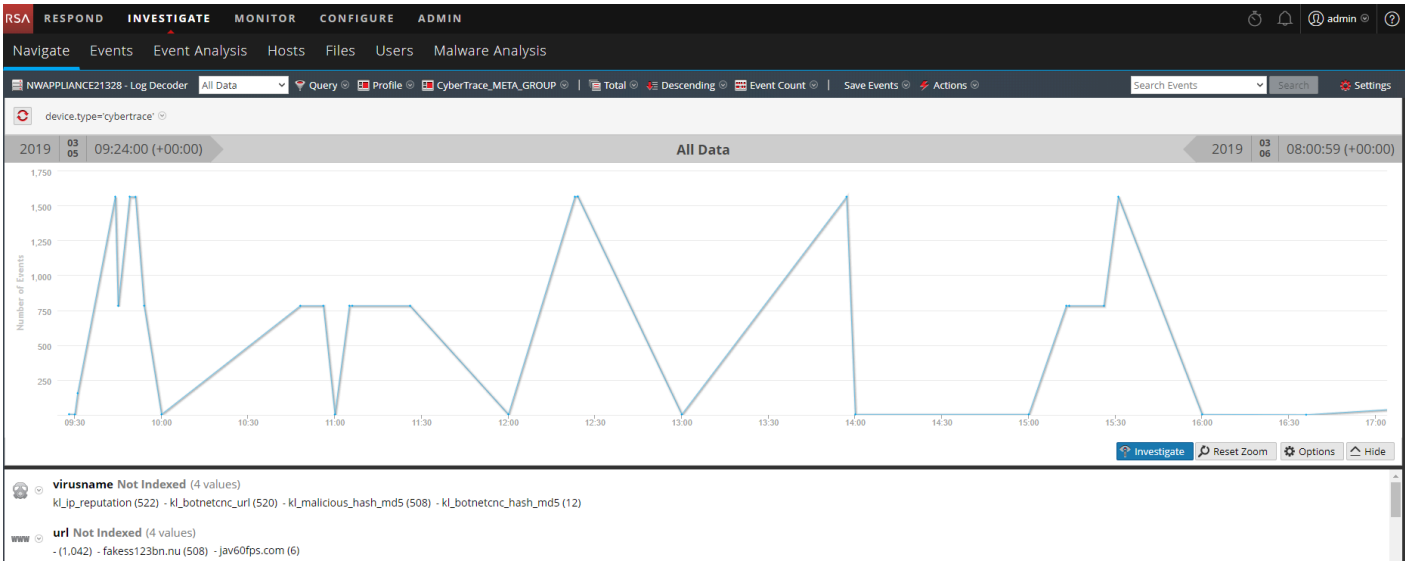
```
device.type='cybertrace'
```



Указание типа устройства

6. Нажмите на кнопку **OK**.

На экране **Navigate** отображаются события из Kaspersky CyberTrace Service.



Отображение событий из Kaspersky CyberTrace Service

Создание и просмотр отчетов

В этом разделе описывается порядок создания и просмотра отчетов в RSA NetWitness. Порядок импорта существующего отчета в RSA NetWitness описывается в разделе Импорт предварительно настроенного отчета в RSA NetWitness.

Чтобы создать новый отчет в RSA NetWitness, выполните следующие действия:

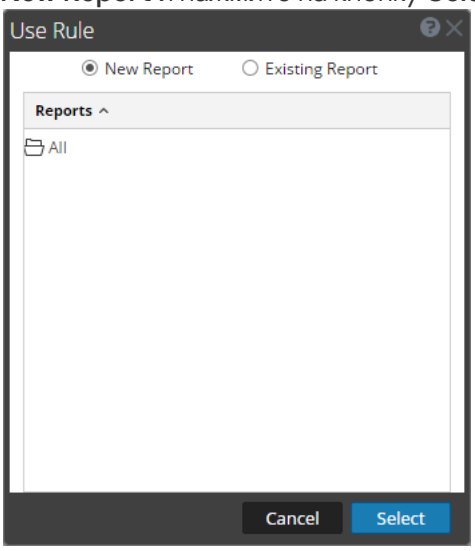
1. В меню RSA NetWitness выберите **Dashboard** → **Reports**. (В RSA NetWitness 11 выберите **Monitor** → **Reports**; в RSA NetWitness 11.6.0 выберите **Reports**).

   Откроется вкладка **Manage**.

2. Выберите правило, на основе которого создается отчет (например, `CyberTrace Detect Botnet`).

3. Для выбранного правила нажмите на кнопку **Settings** (), затем выберите **Create Report**.

4. В окне **Use Rule** выберите вариант **New Report** и нажмите на кнопку **Select**.



Окно **Use Rule**

5. На вкладке **New Report** выберите способ отображения данных.

   Для правила `CyberTrace Detect Botnet` данные можно отображать только в табличной форме.

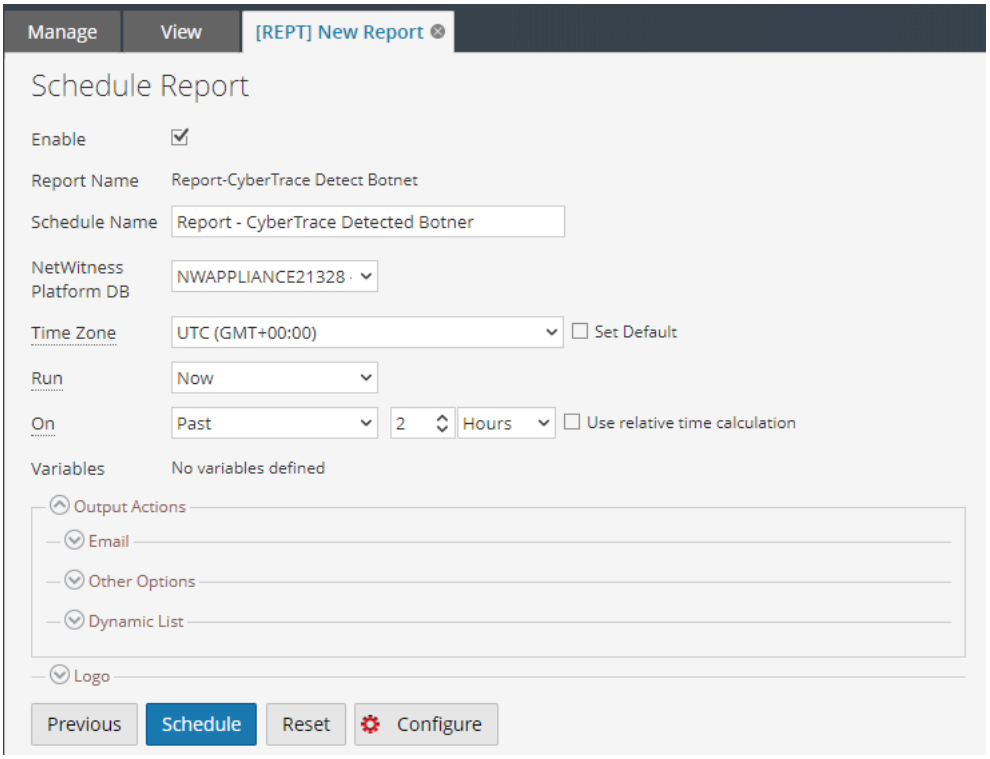
6. Нажмите на кнопку **Schedule**.

   Откроется форма **Schedule Report**.

7. В форме **Schedule Report** укажите следующие данные:

   - Имя расписания.
   - Источник данных (база данных из раскрывающегося списка **NetWitness Platform DB**).
   - Время, когда должен формироваться отчет.

- Период, в течение которого поступают отображаемые данные.
- Действия, которые необходимо выполнить с отчетом (например, отправить его по электронной почте).



Форма «Schedule Report»

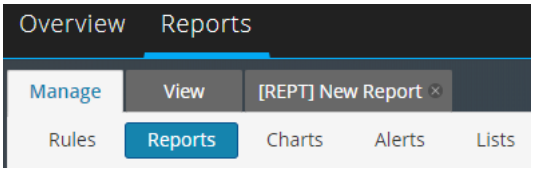
8. Нажмите на кнопку **Schedule**.

Просмотр отчета

Чтобы просмотреть сформированный отчет, выполните следующие действия:

1. В меню RSA NetWitness выберите **Dashboard** → **Reports**. (В RSA NetWitness 11 выберите **Monitor** → **Reports**; в RSA NetWitness 11.6.0 выберите **Reports**).

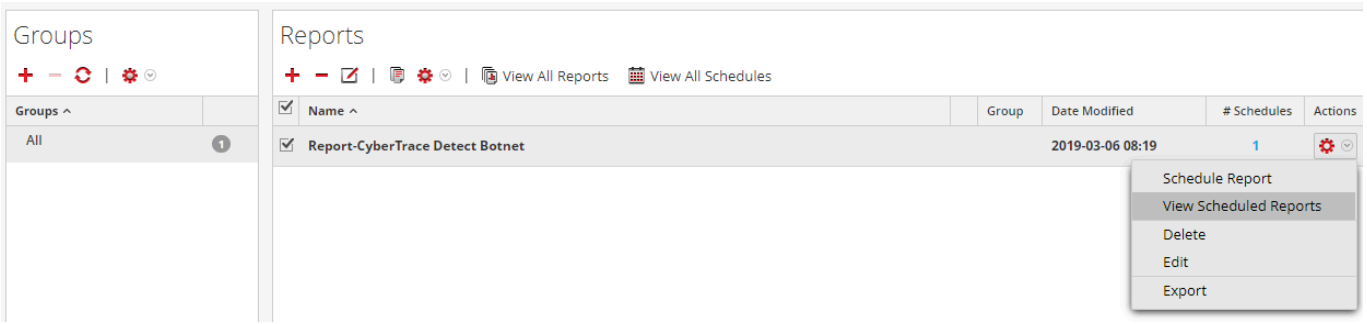
   Откроется вкладка **Manage**.



Вкладка **Manage**

2. Нажмите на кнопку **Reports**.

Отображается экран **Reports**.



Экран **Reports**

3. На панели **Reports** наведите указатель мыши на отчет, нажмите кнопку Settings (), затем выберите **View Scheduled Reports**.

4. Выберите отчет по расписанию, затем нажмите на кнопку **View**.

Создание и просмотр информационных сообщений

В этом разделе описывается порядок создания оповещений в RSA NetWitness.

Чтобы создать новое оповещение в RSA NetWitness, выполните следующие действия:

1. В меню RSA NetWitness выберите **Dashboard** → **Reports**. (В RSA NetWitness 11 необходимо выбрать **Monitor** → **Reports**).

   Откроется вкладка **Manage**.

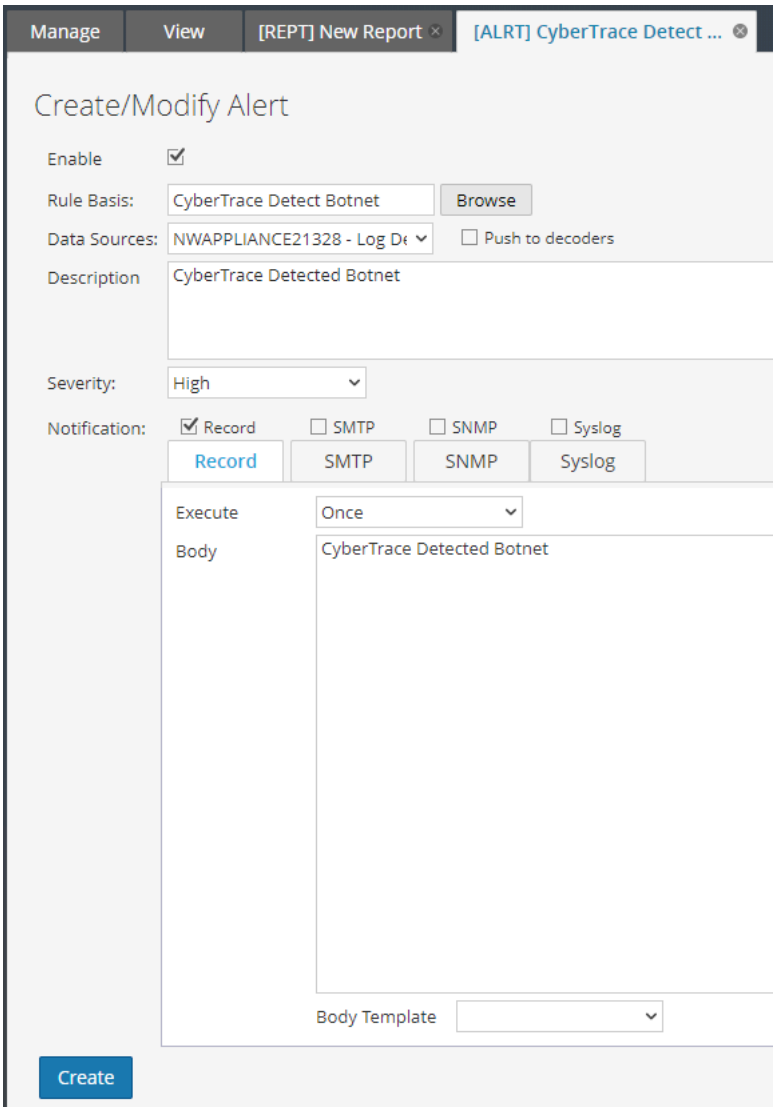
2. Выберите правило, на основе которого создается отчет (например, `CyberTrace Detect Botnet`).

3. Для выбранного правила нажмите на кнопку **Settings** (), затем выберите **Create Alert**.

4. В форме **Create/Modify Alert** укажите следующие данные:

   - Источник данных
   - Описание оповещения

- Уровень важности оповещения
- Тип уведомления (например, можно отправлять уведомления по электронной почте)



Форма **Create/Modify Alert**

5. Нажмите на кнопку **Создать**.

Просмотр оповещений

Чтобы просмотреть оповещение, выполните следующие действия:

1. В меню RSA NetWitness выберите **Dashboard** → **Reports**. (В RSA NetWitness 11 необходимо выбрать **Monitor** → **Reports**).

   Откроется вкладка **Manage**.

2. Нажмите на кнопку **Alerts**.

   Отображается экран **Alert**.

3. На панели инструментов **Alert** нажмите кнопку **View Alerts**.

   Откроется вкладка **View Alerts**.

Создание информационной панели

В этом разделе описывается порядок создания информационной панели в RSA NetWitness с помощью правил Kaspersky CyberTrace Service.

Чтобы создать информационную панель в RSA NetWitness, выполните следующие действия:

1. В меню RSA NetWitness выберите **Dashboard** → **Reports**. (В RSA NetWitness 11 выберите **Monitor** → **Reports**).

2. Выберите правило, используемое для создания отчета (например, отчет `CyberTrace Top 10 URLs`).

3. Для выбранного правила нажмите на кнопку **Settings** (), затем выберите действие **Create Chart**.

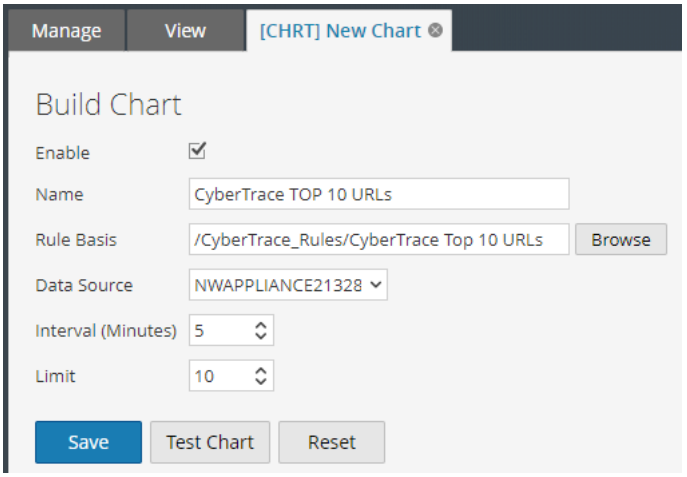
   Откроется окно **Build Chart**.

4. Задайте следующие параметры:

   - Название диаграммы
   - Источник данных

     Укажите источник данных, выдающий события Kaspersky CyberTrace Service.
   - Период обновления
   - Лимит данных

     Например, для диаграмм, содержащих топ-10 объектов, укажите `10`.



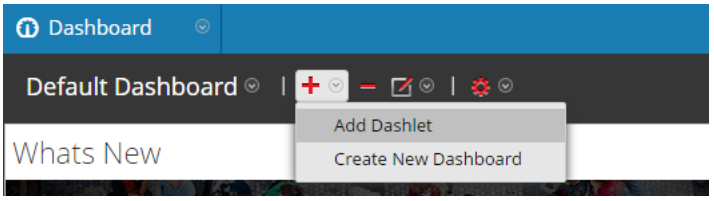
Окно **Build Chart**

5. Нажмите на кнопку **Save**.

6. Активируйте форму **Dashboard**. (В RSA NetWitness 11 вместо этого выберите **Monitor** → **Overview**).

7. Действие, выполняемое на этом шаге, зависит от версии RSA NetWitness.

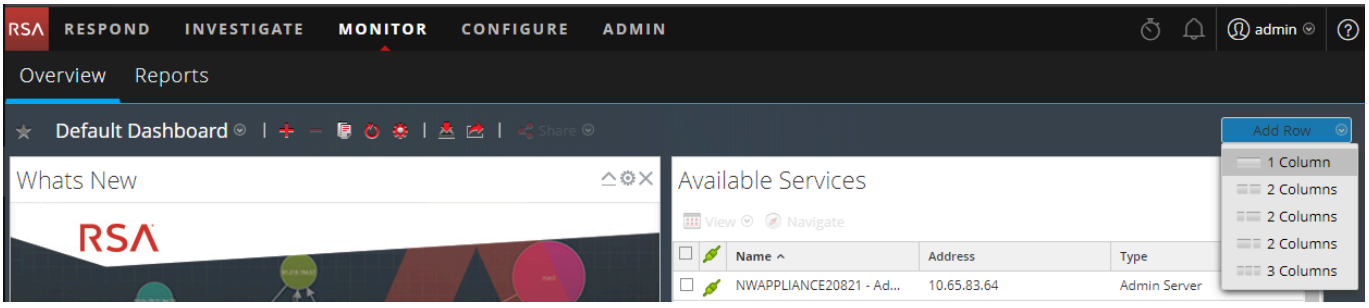
- В RSA NetWitness 10 нажмите кнопку **New** ( ), затем выберите **Add Dashlet**.



Окно **Adding a dashlet**

- В RSA NetWitness 11 выполните следующие действия:

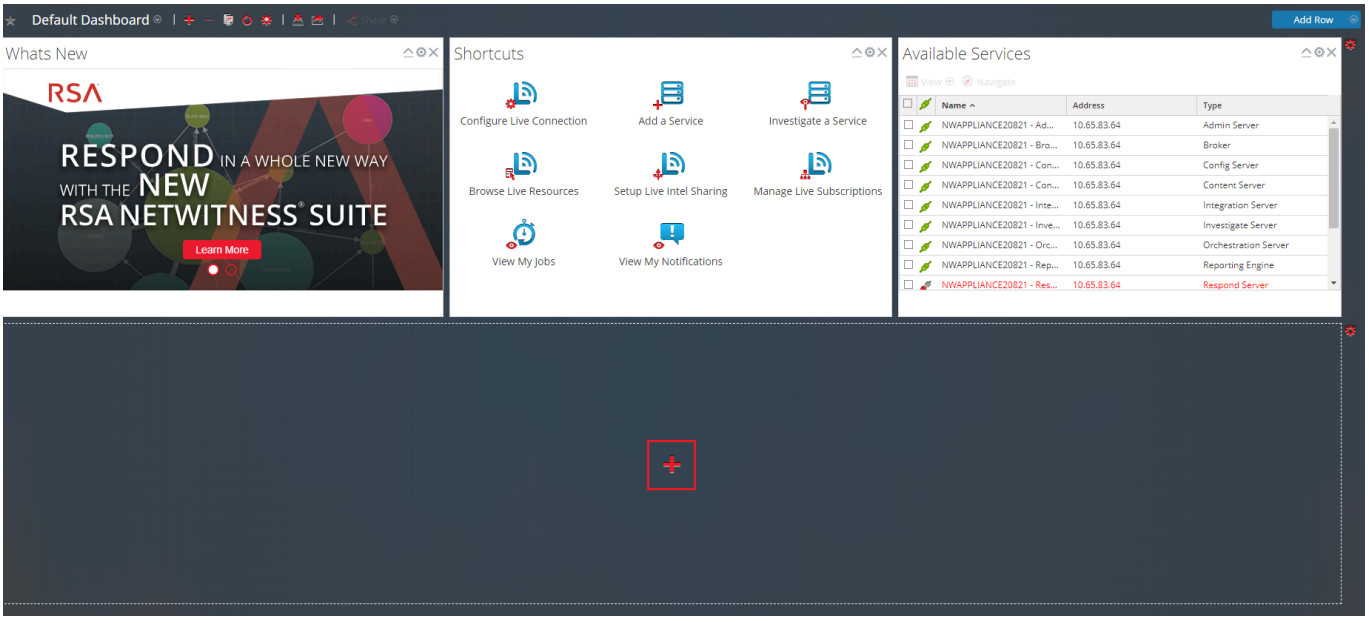
  a. Нажмите на кнопку **Add Row**, затем выберите требуемый тип новой строки.



Добавление строки

a. В появившейся ячейке нажмите на кнопку **Add Dashlet** ( ).

   На рисунке ниже ячейка обведена пунктирной линией.

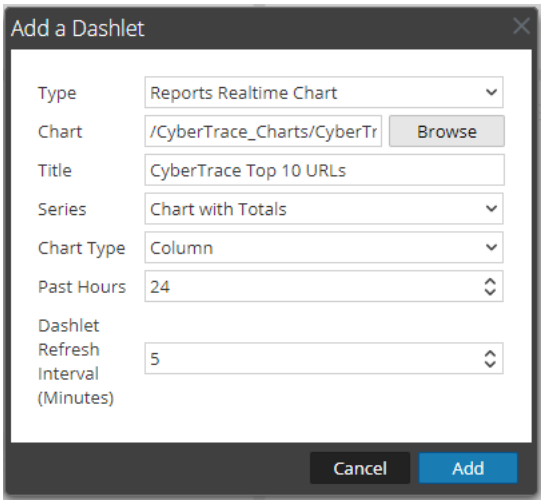


Добавление элемента информационной панели

Откроется окно **Add a Dashlet**.

8. Укажите следующую информацию:

   - Тип элемента информационной панели `Reports Realtime Chart`
   - Отображаемая диаграмма (в данном случае `CyberTrace Top 10 URLs`)
   - Имя элемента информационной панели
   - Тип диаграммы (в данном случае — столбец)
   - Период до настоящего момента, в течение которого подготавливаются данные для отображения
   - Период обновления элемента информационной панели



Окно **Add a Dashlet**

9. Нажмите на кнопку **Добавить**.

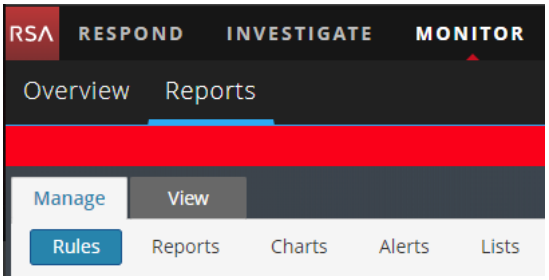
Создание уведомлений о входящих служебных событиях

Для создания уведомлений о входящих служебных событиях Kaspersky CyberTrace можно настроить правила оповещений.

Чтобы создать уведомления о служебных событиях от Kaspersky CyberTrace в RSA NetWitness, выполните следующие действия:

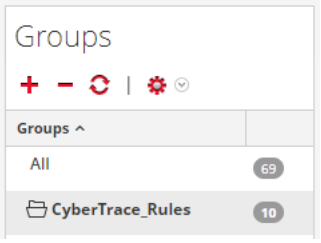
1. В меню RSA NetWitness выберите **Monitor** → **Reports**, затем выберите **Manage** → **Rules**.

   В RSA NetWitness версии 11.6.0 выберите пункт меню **Reports**.



Форма **Manage** → **Rules**

2. В разделе **Groups** выберите **CyberTrace_Rules**.



Правила CyberTrace

3. В разделе **Rules** нажмите на кнопку **Add** ( ). В раскрывающемся списке выберите **NetWitness Platform DB**.

   Откроется окно **Build Rule**.

4. В окне **Build Rule** укажите следующие настройки:

   - В разделе **Name** укажите имя правила.

     Указываемое имя может быть любым.

   - В поле **Summarize** укажите значение, отличное от `None`, если требуется агрегировать события.

   - В поле **Select** укажите поля, которые содержат значения, используемые в уведомлениях.

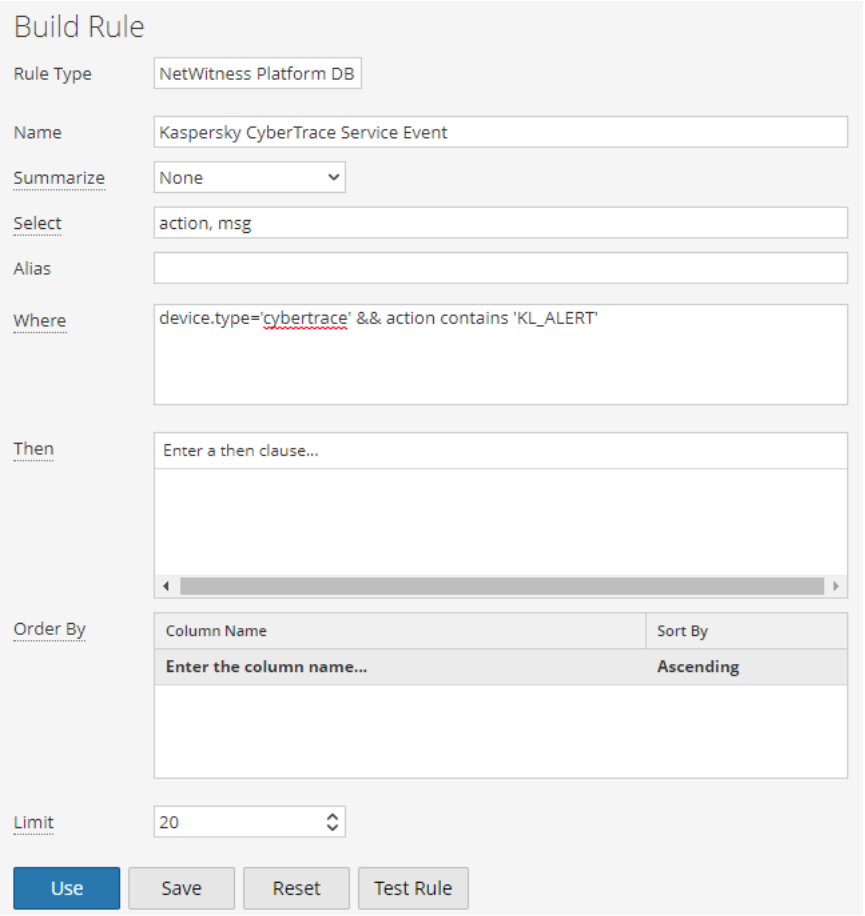
     В служебных событиях Kaspersky CyberTrace используются поля **msg** и **action**.

   - В поле **where** укажите условия уведомления. Например:

     ```
     device.type='cybertrace' && action contains 'KL_ALERT'
     ```

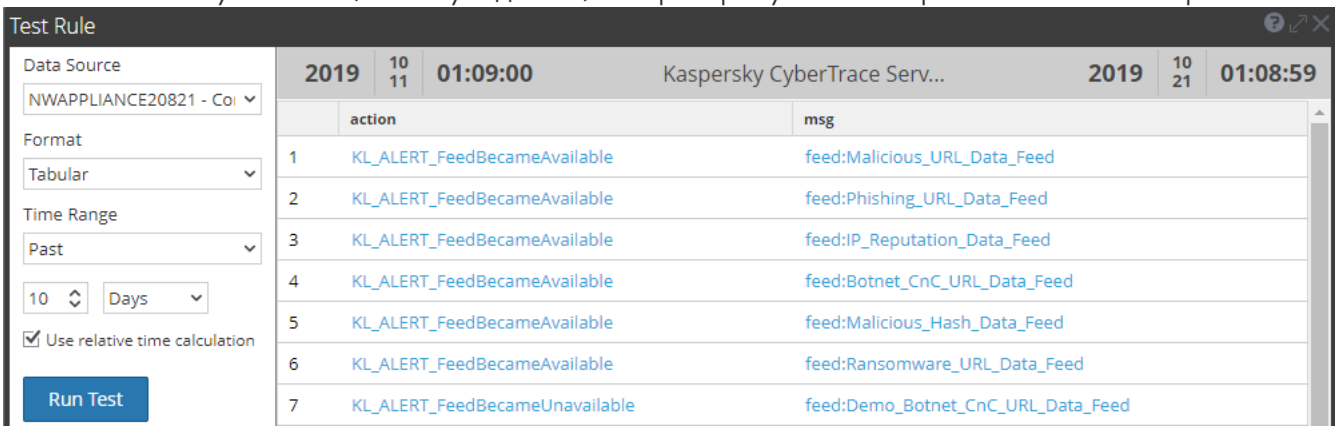
Это условие содержит все служебных события Kaspersky CyberTrace.

- При необходимости заполните остальные поля по своему усмотрению.



Окно **Build Rule**

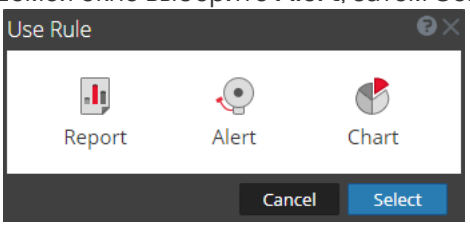
5. Нажмите на кнопку **Test Rule**, чтобы убедиться, что проверка указанных правил выполняется правильно.



Окно **Test Rule**

6. Нажмите на кнопку **Save**, чтобы сохранить правило.

7. Нажмите на кнопку **Use** и в открывшемся окне выберите **Alert**, затем **Select**.



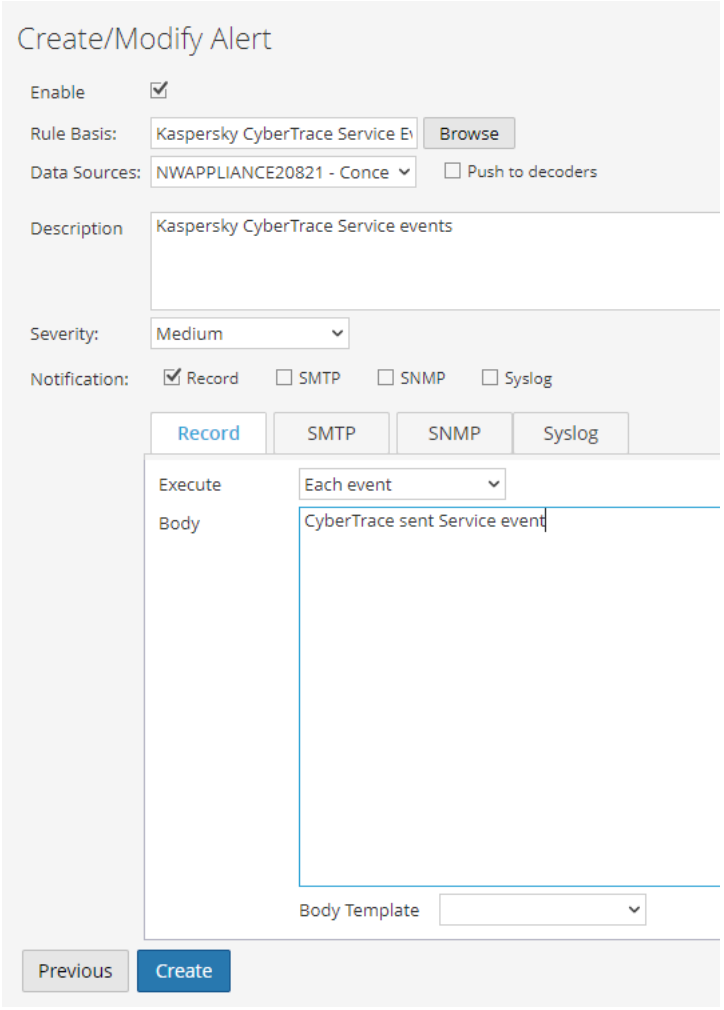
Окно **Use Rule**

Откроется окно **Create/Modify Alert**.

8. В окне **Create/Modify Alert** укажите следующие настройки:

- В поле **Data Source** выберите источник событий с событиями Kaspersky CyberTrace.
- В поле **Description** укажите описание информационного сообщения.

  Указываемое описание может быть любым.
- В поле **Severity** укажите уровень важности оповещения.
- В поле **Notification** укажите следующие настройки:
  - Способ, которым RSA NetWitness будет отправлять уведомления об оповещениях.
  - Тело оповещения.



Окно **Create/Modify Alert**

9. Нажмите на кнопку **Create**, чтобы сохранить правило.

   Правило добавляется в список **Alert** на вкладке **Manage** → **Alerts**.

10. Чтобы просмотреть все предупреждения, удовлетворяющие созданному правилу, нажмите на кнопку **View Alerts** (View Alerts).

Об информационной панели Kaspersky CyberTrace

В этом разделе описывается информационная панель Kaspersky CyberTrace. Эта информационная панель отображается в RSA NetWitness после импорта файла Kaspersky+CyberTrace.cfg.

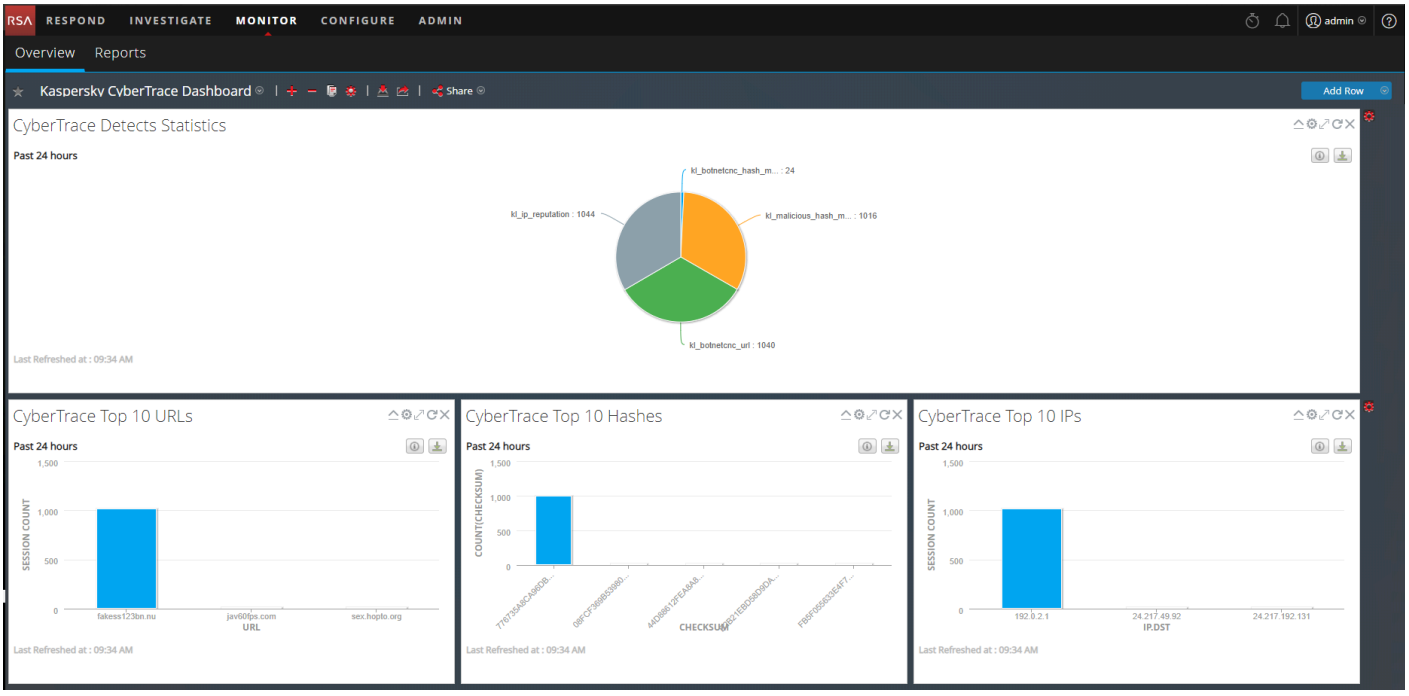
Информационная панель Kaspersky CyberTrace содержит следующие элементы:

- Элемент информационной панели со статистикой обнаружений киберугроз за предыдущие 24 часа
- Элементы информационной панели с топ-10 URL, топ-10 IP-адресов и топ-10 хешей за последние 24 часа
- Элемент информационной панели с служебными событиями из Kaspersky CyberTrace Service за последние 24 часа

  Чтобы указать источник данных для этого элемента информационной панели, нажмите на кнопку **Settings** (), затем выберите **Service**.

- IP-адреса устройств, сгенерировавших события, которые Kaspersky CyberTrace Service преобразовывал в события обнаружения киберугроз в течение последних 24 часов.

Чтобы указать источник данных для этого элемента информационной панели, нажмите на кнопку **Settings** ( ), затем выберите **Service**.



Информационная панель Kaspersky CyberTrace

Руководство по Log Scanner

Утилита Log Scanner — это приложение командной строки, позволяющее отправлять данные в Kaspersky CyberTrace Service для проверки по потоками данных об угрозах. Хеши, IP-адреса и URL можно проверять по одному или в пакетном режиме (в виде файла).

В этой главе объясняется порядок работы с утилитой Log Scanner.

Параметры командной строки

В Linux утилита Log Scanner запускается из командной строки следующим образом:

```
./log_scanner [-h|--help] [-r|--report] [-c|--config] [[-p|--path]|[-s|--hash]|[-u|--url]|[-i|--ip]] [значение]
```

В Windows утилита Log Scanner запускается из командной строки следующим образом:

```
log_scanner.exe [-h|--help] [-r|--report] [-c|--config] [[-p|--path]|[-s|--hash]|[-u|--url]|[-i|--ip]] [значение]
```

Параметры командной строки описаны в следующей таблице.

Параметры командной строки Log Scanner

Параметр	Описание
`-h` `--help`	Вывод на экран сообщения о порядке использования. Если указан этот параметр, все остальные параметры игнорируются.
`-r` `--report`	Если указан этот параметр, Kaspersky CyberTrace Service возвращает ответ в Log Scanner в том же сокете, в котором был отправлен запрос, а Log Scanner сохраняет результат в текстовом файле. Выходному файлу присваивается имя `log_scanner_report%current_time%.txt`, где `%current_time%` – дата и время (включая секунды) создания выходного файла. Место сохранения выходного файла задается в элементе `OutputDir` конфигурационного файла Log Scanner. Если в потоках данных об угрозах Kaspersky Threat Data Feeds обнаружен URL, IP-адрес или хеш, в выходной файл записывается его категория и контекстная информация. После обработки всего ввода на вывод выдается следующая информация: • Количество запросов, отправленных в Kaspersky CyberTrace Service • Количество обнаружений киберугроз, полученных из Kaspersky CyberTrace Service • Время, затраченное на выполнение всех проверок Если этот параметр не указан, Kaspersky CyberTrace Service будет генерировать вывод в соответствии с параметрами, указанными в его конфигурационном файле. Если этот параметр указан, убедитесь, что атрибут `enable` элемента `OutputSetting` → `FinishedEventFormat` в конфигурационном файле Kaspersky CyberTrace Service не имеет значение `false`.
`-c` `--config`	Путь к конфигурационному файлу. Это может быть как абсолютный, так и относительный путь. Относительный путь рассчитывается относительно каталога, из которого запускается Log Scanner. По умолчанию Log Scanner использует конфигурационный файл log_scanner.conf, размещенный в каталоге, из которого запускается Log Scanner.

`-p`
`--path`
	Путь к каталогу или текстовому файлу, содержащему URL, IP-адреса и хеши, которые необходимо сверить с потоками данных Kaspersky Threat Data Feeds. Это может быть как абсолютный, так и относительный путь. Относительный путь рассчитывается относительно каталога, в котором находится исполняемый файл Log Scanner. Если указан путь к каталогу, обрабатываются все файлы, содержащиеся в нем и во всех его подкаталогах.
	Каждая строка каждого обработанного файла отправляется в Kaspersky CyberTrace Service в качестве данных для проверки. Какое-либо дополнительное форматирование не применяется. Kaspersky CyberTrace Service анализирует строки с использованием регулярных выражений, заданных в его конфигурационном файле.
	Можно указать несколько путей; в этом случае каждый путь следует предварять ключом `-p`. Например:
	`./log_scanner -p log1.txt -p log2.txt`
	`log_scanner.exe -p log1.txt -p log2.txt`

`-s`
`--hash`
	Хеши, которые необходимо сверить с потоками данных Kaspersky Threat Data Feeds. Это могут быть хеши MD5, SHA1 или SHA256; Log Scanner определяет тип хеша по его длине. Если указывается несколько хешей, они должны быть разделены символами пробела. Например:
	`./log_scanner -s A8315A5D4C8ACB982372C16B83BAEAAA -s A72C5B99F2706B00718279C9533A3648`
	`log_scanner.exe -s A8315A5D4C8ACB982372C16B83BAEAAA -s A72C5B99F2706B00718279C9533A3648`

`-i`
`--ip`
	IP-адреса, которые необходимо сверить с потоками данных Kaspersky Threat Data Feeds. Если указывается несколько IP-адресов, они должны быть разделены символами пробела. Например:
	`./log_scanner -i 15.54.33.54 -i 45.62.66.69`
	`log_scanner.exe -i 15.54.33.54 -i 45.62.66.69`

`-u`
`--url`
	URL, которые необходимо сверить с потоками данных Kaspersky Threat Data Feeds. Если указывается несколько URL, они должны быть разделены символами пробела. Например:
	`./log_scanner -u http://example.com/malware_test -u http://example.com/phishing_test`
	`log_scanner.exe -u http://example.com/malware_test -u http://example.com/phishing_test`
	Параметр `-u` не следует использовать для проверки URL, содержащих амперсанд (`&`). Чтобы проверить URL, содержащий амперсанд, скопируйте этот URL в текстовый файл и проверьте этот файл с использованием параметра `-p`, как описано выше.

Если не указан ни один из параметров `-p`, `-s`, `-u` или `-i`, а только значение для проверки, это значение интерпретируется как путь к файлу или каталогу для проверки.

Утилита Log Scanner использует текущую локаль операционной системы.

Примеры сценариев использования

В этом разделе приведены примеры использования Log Scanner в некоторых ситуациях.

Проверка нескольких файлов журналов

Все файлы журналов, передаваемые на проверку, должны быть в кодировке UTF-8. Если файлы журналов имеют другую кодировку, их необходимо преобразовать в UTF-8.

Если есть потоки данных об угрозах, которые еще не были скомпилированы, и каталог, содержащий файлы журнала, можно проверить файлы журнала по следующей процедуре.

Чтобы проверить несколько файлов журналов, выполните следующие действия:

1. В конфигурационном файле kl_feed_service.conf укажите используемые потоки данных об угрозах, правила нормализации для обработки событий в файлах журналов и регулярные выражения для парсинга событий.

2. Запустите Kaspersky CyberTrace Service:

   `systemctl start cybertrace.service` (в Linux)

   `sc start cybertrace` (в Windows)

3. Запустите утилиту Log Scanner и укажите каталог, в котором находятся файлы журналов. Например:

   `./log_scanner –r –p ../logs` (в Linux)

   `log_scanner.exe –r –p ..\logs` (в Windows)

4. Остановите Kaspersky CyberTrace Service следующей командой:

   `systemctl stop cybertrace.service` (в Linux)

   `sc stop cybertrace` (в Windows)

После завершения работы Log Scanner каталог, указанный в элементе `OutputDir` конфигурационного файла log_scanner.conf, будет содержать отчет об URL и хешах, обнаруженных Kaspersky CyberTrace Service.

Проверка нескольких URL и хешей

Если требуется проверить несколько URL и хешей, выполните действия в следующем порядке.

Чтобы проверить несколько URL и хешей, выполните следующие действия:

1. Запустите Kaspersky CyberTrace Service следующей командой:

   `systemctl start cybertrace.service` (в Linux)

   `sc start cybertrace` (в Windows)

2. Запустите Log Scanner и укажите хеши для проверки. Например:

   `./log_scanner –r –s A72C5B99F2706B00718279C9533A3648 -s 6AA0321FA9D82D652AB53882D7CF9E592B4439B8` (в Linux)

   `log_scanner.exe –r –s A72C5B99F2706B00718279C9533A3648 -s 6AA0321FA9D82D652AB53882D7CF9E592B4439B8` (в Windows)

3. Запустите Log Scanner и укажите URL для проверки. Например:

   `./log_scanner –r –u test.mav.example.com?bad_url=1 -u test.phishing.example.com/psh/test?p=1&p=2` (в Linux)

   `log_scanner.exe –r –u test.mav.example.com?bad_url=1 -u test.phishing.example.com/psh/test?p=1&p=2` (в Windows)

4. Остановите Kaspersky CyberTrace Service следующей командой:

   `systemctl stop cybertrace.service` (в Linux)

   `sc stop cybertrace` (в Windows)

После завершения работы Log Scanner каталог, указанный в элементе `OutputDir` конфигурационного файла log_scanner.conf, будет содержать отчет об URL, обнаруженных Kaspersky CyberTrace Service, и отчет об обнаруженных хешах.

Конфигурационный файл (Log Scanner)

Конфигурационный файл Log Scanner представляет собой XML-файл, содержащий параметры, описанные в таблице ниже. Если этого файла нет в каталоге или в нем отсутствуют некоторые параметры, для отсутствующих параметров используются значения по умолчанию.

Параметры конфигурационного файла

Параметр	Описание
`Verbose`	Регулирует количество информации, которую Log Scanner выводит в консоль. Если элемент `Verbose` имеет значение `False` или `0` или элемент не указан, в консоль выводится малое количество информации. В противном случае выводится подробная информация.
`ThreadsCount`	Максимальное количество потоков, которые Log Scanner может использовать при обработке входных данных. По умолчанию используется до 8 потоков.
`OutputDir`	Каталог, в котором будет находиться выходной файл. Это может быть как абсолютный, так и относительный путь. Относительный путь рассчитывается относительно каталога, в котором находится исполняемый файл Log Scanner. Если параметр `OutputDir` не задан, выходной файл сохраняется в каталоге, где находится исполняемый файл Log Scanner.
`Pattern`	Утилита отправляет запросы в Kaspersky CyberTrace Service в формате, указанном в элементе `Pattern`. Можно использовать следующие параметры: • `%IP%` — значение, которое необходимо проверить, если утилита вызывается с параметром `-i` (`--ip`). • `%MD5%`, значение, которое необходимо проверить, если утилита вызывается с параметром `-s` (`--hash`) и значение является хешем MD5. • `%SHA1%` — значение, которое необходимо проверить, если утилита вызывается с параметром `-s` (`--hash`) и значение является хешем SHA1. • `%SHA256%` — значение, которое необходимо проверить, если утилита вызывается с параметром `-s` (`--hash`) и значение является хешем SHA256. • `%URL%` — значение, которое необходимо проверить, если утилита вызывается с параметром `-u` (`--url`). По умолчанию используется следующее значение: `ip=%IP% md5=%MD5% sha1=%SHA1% sha256=%SHA256% url=%URL%`
`Connection`	Задает IP-адрес и порт (или именованный канал Windows или сокет UNIX), на который Log Scanner будет отправлять полученные данные. • Если используется какая-либо неподдерживаемая SIEM-система, параметр `Connection` должен задавать способ подключения к этой системе. • Если SIEM-система не используется, параметр `Connection` должен задавать способ подключения к Kaspersky CyberTrace Service. Значение зависит от способа, которым Log Scanner взаимодействует с SIEM-системой или с Kaspersky CyberTrace Service. • Если они взаимодействуют по протоколу TCP/IP, укажите в элементе `Connection` IP-адрес и порт, на которые Kaspersky CyberTrace Service получает события. • Если они взаимодействуют через именованный канал Windows, укажите в элементе `Connection` именованный канал, по которому Kaspersky CyberTrace Service получает события. Имя канала должно быть указано в формате `\\.\pipe\<pipe_name>`. • Если они взаимодействуют через сокет UNIX, укажите в элементе `Connection` сокет, через который служба Feed получает события. По умолчанию данные отправляются на `127.0.0.1:9999`.
`SocketTimeout`	Количество секунд, в течение которых Log Scanner ожидает, пока сокет или канал, указанный в параметре `Connection`, возобновит отправку данных. Если значение этого параметра равно `0`, Log Scanner ожидает бесконечно. Максимальное допустимое значение этого параметра равно `1000`. По умолчанию время ожидания равно 15 секундам.

Пример конфигурационного файла

```
<Settings>
	<Verbose>0</Verbose>
	<ThreadsCount>8</ThreadsCount>
	<OutputDir>../log_scanner_reports</OutputDir>
	<Pattern>ip=%IP% md5=%MD5% sha1=%SHA1% sha256=%SHA256% url=%URL%</Pattern>
	<Connection>127.0.0.1:9999</Connection>
	<SocketTimeout>15</SocketTimeout>
</Settings>
```

Рекомендации по использованию Log Scanner

Рекомендуется использовать Kaspersky CyberTrace Service вместе с Log Scanner в следующих случаях:

- Необходимо проверить несколько файлов журналов и сохранить результат проверки в файл.

  Это может быть удобно при расследовании инцидентов информационной безопасности, когда используемая SIEM-система недоступна или SIEM-системы не используются.

- Необходимо проверить несколько файлов журналов и отправить результаты проверки в используемую SIEM-систему.

Настройка Kaspersky CyberTrace Service и Log Scanner

Kaspersky CyberTrace Service и Log Scanner должны взаимодействовать правильным образом, поэтому необходимо обеспечить взаимное соответствие их параметров:

- Порт, заданный в элементе `Settings > Connection` конфигурационного файла Log Scanner, должен соответствовать порту, указанному в элементе `InputSettings > ConnectionString` конфигурационного файла Kaspersky CyberTrace Service.

- Количество потоков, указанное в элементе `Settings > ThreadsCount` конфигурационного файла Log Scanner, должно быть меньше, чем количество, указанное в элементе `ServiceSettings > ScannersCount` конфигурационного файла Kaspersky CyberTrace Service.

- Данные, отправляемые Log Scanner в Kaspersky CyberTrace Service — либо строки файлов журналов, либо строки, созданные на основе элемента конфигурационного файла Log Scanner `Settings > Pattern` — должны поддаваться парсингу с помощью регулярных выражений, указанных в элементе `Configuration > InputSettings > RegExps` конфигурационного файла Kaspersky CyberTrace Service.

Примеры конфигурационных файлов

Ниже приведен отрывок из примера конфигурационного файла Kaspersky CyberTrace Service.

```
<Configuration>
    <InputSettings>
        <RegExps>
            <Source id="default">
                <!--You can use them in the OutputSettings->EventFormat string with the pattern %REGEXPNAME%-->
                ...
                <RE_MD5>md5=(.*?)(?:$|\s)</RE_MD5>
                <RE_SHA1>sha1=(.*?)(?:$|\s)</RE_SHA1>
                <RE_SHA256>sha256=(.*?)(?:$|\s)</RE_SHA256>
                <RE_URL>url=(.*?)(?:$|\s)</RE_URL>
                <RE_IP>ip=(.*?)(?:$|\s)</RE_IP>
            </Source>
        </RegExps>
        <ConnectionString>127.0.0.1:9999</ConnectionString> <!-- <ip>:<port>. Threat Feed Service listens for
<ip>:<port>. <port> must be available -->
    </InputSettings>

    <Feeds per_scan_detect_limit="10000">...</Feeds>

    <OutputSettings>
        ...
        <FinishedEventFormat>LookupFinished</FinishedEventFormat>
    </OutputSettings>

    <ServiceSettings>
        ...
        <ScannersCount>9</ScannersCount> <!-- 1 tcp connection = 1 scanner -->
    </ServiceSettings>
</Configuration>
```

Ниже приведен отрывок из конфигурационного файла Log Scanner, который соответствует конфигурационному файлу Kaspersky CyberTrace Service, приведенному выше.

```
<Settings>
        ...
        <ThreadsCount>8</ThreadsCount>
        <Pattern>ip=%IP% md5=%MD5% sha1=%SHA1% sha256=%SHA256% url=%URL%</Pattern>
        <Connection>127.0.0.1:9999</Connection>
</Settings>
```

При использовании этих конфигурационных файлов Log Scanner отправляет запросы на IP-адрес 127.0.0.1 и порт 9999, а Kaspersky CyberTrace Service прослушивает порт 9999 для получения данных на проверку. Как Log Scanner, так и Kaspersky CyberTrace Service используют до восьми потоков для передачи и обработки данных (Kaspersky CyberTrace Service использует один из потоков для механизма проверки работоспособности). Если в Kaspersky CyberTrace Service отправляются корректные URL, IP-адреса и хеши, они будут проходить парсинг с использованием регулярных выражений, указанных в конфигурационном файле Kaspersky CyberTrace Service.

Работа с результатами проверки

После того, как данные будут проверены Kaspersky CyberTrace Service, можно отправить результаты проверки в целевое программное обеспечение или сохранить их в файл:

- Для отправки результатов проверки в целевое программное обеспечение задайте правильное значение элемента `OutputSettings` > `ConnectionString` в конфигурационном файле Kaspersky CyberTrace Service.

- Чтобы сохранить результаты проверки в файл, передайте параметр `-r` при запуске Log Scanner из командной строки следующим образом:

  `./log_scanner -r -p file_to_check` (в Linux)

  `log_scanner.exe -r -p file_to_check` (в Windows)

Значение атрибута `enable` элемента `OutputSettings > FinishedEventFormat` в конфигурационном файле Kaspersky CyberTrace Service не должно быть `false`.

Пример отчета

Содержание отчета зависит от значения элемента `OutputSettings > EventFormat` в конфигурационном файле Kaspersky CyberTrace Service.

Ниже приведен пример отчета, отправляемого из Kaspersky CyberTrace Service в Log Scanner.

```
- KL_Data_Feed_Service_v1 LEEF:1.0|Kaspersky Lab|SIEM
Service|1.0|KL_Malicious_URL|url=malicious_domain_21.com/folder/load.php?| IP=91.202.63.117, 196.254.10.200,
194.190.253.19, 185.56.137.11, 178.62.5.157, 173.194.222.211, 159.253.145.183, 87.250.250.135, 82.145.209.252,
74.125.205.211 first_seen=11.01.2016 07:17 geo=ru, ua, kz, by, de, ro, az, cz, uz, md id=9491494
last_seen=14.01.2016 13:36 mask=malicious_domain_21.com/folder/load.php?* popularity=5 type=21
Total number of objects sent to KTFS: 1
Total number of detects received from KTFS: 1
Total scan time: 00:00:01.032
```

Руководства администратора

В этой главе представлена информация об использовании веб-интерфейса Kaspersky CyberTrace, инструментов командной строки и приложений для SIEM-систем.

Работа с веб-интерфейсом Kaspersky CyberTrace

В этом разделе описывается управление Kaspersky CyberTrace пользователями с различными ролями через веб-интерфейс пользователя (веб-интерфейс).

Работа с предустановленной учетной записью

В этом разделе объясняется порядок работы с предустановленными учетными записями и паролями для других пользователей.

Предустановленная учетная запись

После установки Kaspersky CyberTrace для веб-интерфейса Kaspersky CyberTrace задана следующая предустановленная учетная запись:

- Имя пользователя: `admin`
- Пароль: `CyberTrace!1`

Чтобы избежать возможных угроз безопасности, следует как можно скорее изменить этот пароль.

Сброс пароля для предустановленного пользователя

Чтобы сбросить учетные данные для предустановленного пользователя (`admin`), воспользуйтесь утилитой kl_access_util.

Смена паролей для других пользователей

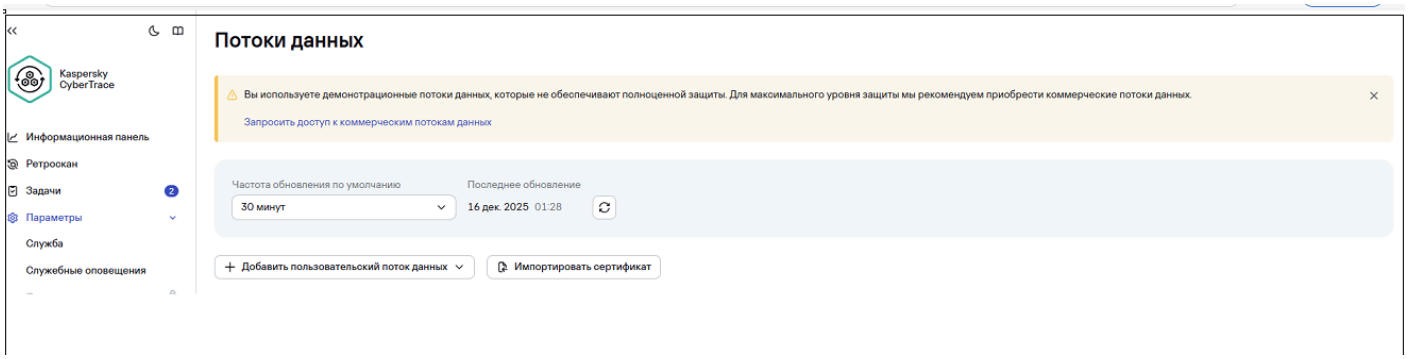
Чтобы создать учетные записи и изменить пароли для других пользователей, воспользуйтесь страницей **Параметры → Пользователи**.

Уведомления веб-интерфейса Kaspersky CyberTrace

Уведомления отображаются в веб-интерфейсе Kaspersky CyberTrace при возникновении вероятных проблем или ограничений в работе Kaspersky CyberTrace. В этом разделе содержится информация о подобных уведомлениях и рекомендуемых действиях, которые должен выполнить администратор.

Уведомление о демонстрационных потоках данных об угрозах

При использовании Kaspersky CyberTrace на уровне лицензирования Community Edition доступны только демонстрационные потоки данных об угрозах. В этом случае в веб-интерфейсе Kaspersky CyberTrace отображается уведомление на странице **Параметры** → **Потоки данных** с рекомендацией приобрести коммерческие потоки данных об угрозах для включения максимального уровня защиты.



Уведомление о демонстрационных потоках данных об угрозах

Дополнительная информация о доступных потоках данных об угрозах Kaspersky Data Feed приведена в разделе О потоках данных об угрозах Kaspersky Threat Data Feeds.

Уведомление о свободном месте на жестком диске

При обновлении потоков данных об угрозах Kaspersky CyberTrace проверяет объем свободного места на диске. Если на диске осталось мало места, в веб-интерфейсе Kaspersky CyberTrace отображается уведомление. В уведомлении указывается, сколько места на диске в мегабайтах еще доступно для базы данных индикаторов. Кроме того, Kaspersky CyberTrace отправляет оповещение KL_ALERT_FreeSpaceEnds.

Если в веб-интерфейсе Kaspersky CyberTrace выводится это уведомление, можно установить дополнительные жесткие диски или отключить избыточные потоки данных об угрозах.

Дополнительные сведения о необходимом пространстве на жестком диске приведены в разделе Аппаратные и программные требования.

Уведомление об изменении лицензионного ключа

Когда в Kaspersky CyberTrace меняется активный лицензионный ключ, в Kaspersky CyberTrace отображается уведомление и генерируется оповещение `KL_ALERT_LicenseChanged`.

Подробнее о лицензионных ключах сообщается в разделе О лицензировании.

Уведомление об истечении срока действия лицензионного ключа

Когда истекает срок действия лицензионного ключа, используемого Kaspersky CyberTrace, в веб-интерфейсе Kaspersky CyberTrace отображается уведомление и генерируется оповещение `KL_ALERT_LicenseExpires`.

Если в веб-интерфейсе Kaspersky CyberTrace отображается это уведомление, обратитесь к своему менеджеру по работе с клиентами для получения нового лицензионного ключа.

По истечении срока действия лицензионного ключа в веб-интерфейсе Kaspersky CyberTrace отображается уведомление и генерируется оповещение `KL_ALERT_LicenseExpired`. После этого Kaspersky CyberTrace пытается переключиться на один из дополнительных лицензионных ключей, которые были заблаговременно добавлены на странице **Параметры** → **Лицензирование**. Если дополнительных лицензионных ключей нет, Kaspersky CyberTrace меняет уровень лицензирования на Community Edition, отображает уведомление в веб-интерфейсе Kaspersky CyberTrace и генерирует оповещение `KL_ALERT_LicenseChanged`.

Подробнее о лицензионных ключах сообщается в разделе О лицензировании.

Уведомление о превышении лимита EPS

Kaspersky CyberTrace обрабатывает не больше событий в секунду (EPS), чем разрешено уровнем лицензирования. Если лимит EPS превышен, Kaspersky CyberTrace сначала отображает уведомление в веб-интерфейсе Kaspersky CyberTrace, а затем генерирует оповещение `KL_ALERT_EPSLimitExceeded`, не накладывая ограничений. Затем, если лимит EPS непрерывно превышается в течение семи дней, Kaspersky CyberTrace отображает другое уведомление, генерирует оповещение `KL_ALERT_EPSHardLimit` и ограничивает количество обрабатываемых событий.

Если в веб-интерфейсе Kaspersky CyberTrace отображается это уведомление, можно уменьшить количество обрабатываемых событий или обратиться к менеджеру по работе с клиентами, чтобы изменить уровень лицензирования.

Дополнительные сведения об ограничении EPS приведены в разделе Ограничения, накладываемые лицензионными ключами.

Уведомление о превышении ограничения на количество индикаторов

Это уведомление относится только к уровню лицензирования Community Edition.

Уровень лицензирования устанавливает ограничение на общее количество индикаторов; Kaspersky CyberTrace считывает в сумме не больше записей из всех потоков данных, чем разрешено лицензионным ключом или уровнем лицензирования.

Если количество индикаторов превышает лимит, Kaspersky CyberTrace отправляет событие `KL_ALERT_IndicatorsStoreHardLimit`, а затем отображает в веб-интерфейсе Kaspersky CyberTrace уведомление о наличии ограничения на добавление и обновление индикаторов. При генерации события `KL_ALERT_IndicatorsStoreHardLimit` Kaspersky CyberTrace перестает считывать новые записи.

Если в веб-интерфейсе Kaspersky CyberTrace отображается это уведомление, можно отключить избыточные потоки данных об угрозах или обратиться к менеджеру по работе с клиентами, чтобы изменить уровень лицензирования.

Дополнительные сведения об ограничении общего количества индикаторов приведены в разделе Ограничения, накладываемые лицензионными ключами.

Управление Kaspersky CyberTrace

В этом разделе описывается порядок настройки экземпляра Kaspersky CyberTrace в целом.

Все страницы веб-интерфейса, описанные в этом разделе, доступны только с ролью «Администратор». У пользователей с ролью «Аналитик» или «Менеджер тенанта» нет доступа к этим страницам.

Для работы с веб-страницами, описанными в этом разделе, необходимо перейти в режим **Управление системой**.

Настройки службы

Управлять общими параметрами Kaspersky CyberTrace можно в веб-интерфейсе в разделе **Параметры** → **Служба**. Для работы с этим разделом необходимо перейти в режим **Управление системой**. Этот режим доступен только пользователям с ролью «Администратор».

В разделе **Служба** отображается статус Kaspersky CyberTrace Service. На этой странице можно изменять настройки, которые хранятся в конфигурационных файлах kl_feed_util.conf и kl_feed_service_log.conf. Также здесь можно выполнить ряд действий.

Статус Kaspersky CyberTrace Service

Один из следующих статусов Kaspersky CyberTrace Service status:

- **Kaspersky CyberTrace работает**
- **Kaspersky CyberTrace запускается**

- **Kaspersky CyberTrace прекратил работу**

  Этот статус указывает, что индикаторы загружаются в базу данных и индексируются. Пока все индикаторы не будут обработаны, вкладка **Indicators** может содержать частично устаревшую информацию, а поиск данных, которые находятся в процессе обновления, может выполняться некорректно. Однако процесс сопоставления входящих событий выполняется на основе фактических данных, и на странице веб-интерфейса Kaspersky CyberTrace с подробной информацией об индикаторах отображаются актуальные данные.

Connection settings

На вкладке **Соединение** раздела **Служба** задайте следующие параметры:

1. В разделе **Пороговый EPS системы** настройте пороговый EPS системы (общее число событий в секунду — events per second):

   a. Включите переключатель.

   b. В поле **Пороговый EPS** введите требуемое значение порогового EPS.

   > Если пороговый EPS системы определяется лицензией, в веб-интерфейсе Kaspersky CyberTrace его изменить невозможно.

   > Если не задать пороговый EPS системы, можно столкнуться с непредвиденной деградацией производительности системы.

2. В разделе **Service alerts** настройте отправку служебных оповещений, посредством которых другое ПО (например, SIEM-система) снабжается информацией о состоянии Kaspersky CyberTrace Service. Для этого выполните действия в следующем порядке:

   a. Включите переключатель.

   b. В полях **IP-адрес** и **Порт** укажите параметры сервера, на который требуется отправлять служебные оповещения.

   По умолчанию указаны IP-адрес `127.0.0.1` и порт `9999`.

   > Поддерживается отправка служебных оповещений на адреса IPv6.

   c. В поле **Secure connection** выберите тип соединения: **TLS с проверкой сертификата**, **TLS без проверки сертификата** или **Нет**.

   Эти настройки хранятся в элементе `OutputSettings > AlertConnectionString` файла kl_feed_service.conf.

3. В разделе **Веб-интерфейс** укажите IP-адрес или имя хоста, используемые для подключения к веб-интерфейсу Kaspersky CyberTrace. Это IP-адрес или имя хоста того сервера, на котором установлен Kaspersky CyberTrace и который используется, например, для скачивания отчетов об экспорте индикаторов.

В качестве адреса веб-интерфейса можно использовать адрес IPv6.

Эта настройка хранится в элементе `ResourcesIP` файла kl_feed_service.conf.

По умолчанию указан адрес `127.0.0.1`.

Настройка прокси-сервера

На вкладке **Прокси-сервер** страницы **Служба** задайте следующие параметры:

1. Включите переключатель **Работать через прокси-сервер**.
2. В поле **IP-адрес или имя хоста** укажите IP-адрес или имя хоста прокси-сервера.
   Эта настройка хранится в элементе `Host` файла kl_feed_util.conf.
3. В поле **Порт** укажите порт прокси-сервера.
   Эта настройка хранится в элементе `Port` файла kl_feed_util.conf.
4. Если для доступа к прокси-серверу требуются учетные данные, выполните следующие действия:
   a. Включите переключатель **Использовать учетные данные для подключения к прокси-серверу**.
   b. В поле **Имя пользователя** укажите имя пользователя для доступа к прокси-серверу.
      Эта настройка хранится в зашифрованном виде в элементе `User` файла kl_feed_util.conf.
   c. В поле **Пароль** укажите пароль для доступа к прокси-серверу.
      Эта настройка хранится в зашифрованном виде в элементе `Password` файла kl_feed_util.conf.

Для прокси-сервера можно использовать адрес IPv6.

Положение о Kaspersky Security Network (KSN)

На вкладке **Положение о KSN** в разделе **Служба** вы можете прочитать соглашение, регламентирующее использование Kaspersky Security Network, и принять или отклонить его.

Чтобы выбрать статус Положения о KSN, выполните следующие действия:

1. Внизу поля с текстом Положения о KSN выберите **Я принимаю Положение о KSN** или **Я не принимаю Положение о KSN**.
2. Нажмите на кнопку **Save**.

Статус Положения о KSN будет выбран.

Информацию о Kaspersky Security Network см. в статье Положение о предоставлении данных.

Доступные действия

На странице **Служба** можно выполнять следующие действия:

- **Перезапустить службу**
- **Экспортировать конфигурационный файл**

  Можно экспортировать конфигурационные файлы kl_feed_service.conf и kl_feed_util.conf в выбранный каталог.

- **Выполнить самостоятельную диагностику**

  Проверяется правильность работы используемых потоков данных «Лаборатории Касперского» об угрозах.

  > Самостоятельную диагностику следует запускать перед редактированием каких-либо правил фильтрации для потока данных на странице **Параметры → Потоки данных**.

  Если проверка работоспособности (самостоятельная диагностика) дает неверные результаты (т. е. если поток данных об угрозах, который должен давать обнаружения киберугроз, не дает их), рассмотрите возможные решения проблемы в разделе Устранение общих неполадок. Если проблема не устранена, обратитесь по адресу intelligence@kaspersky.com.

- **Сбросить статистику**

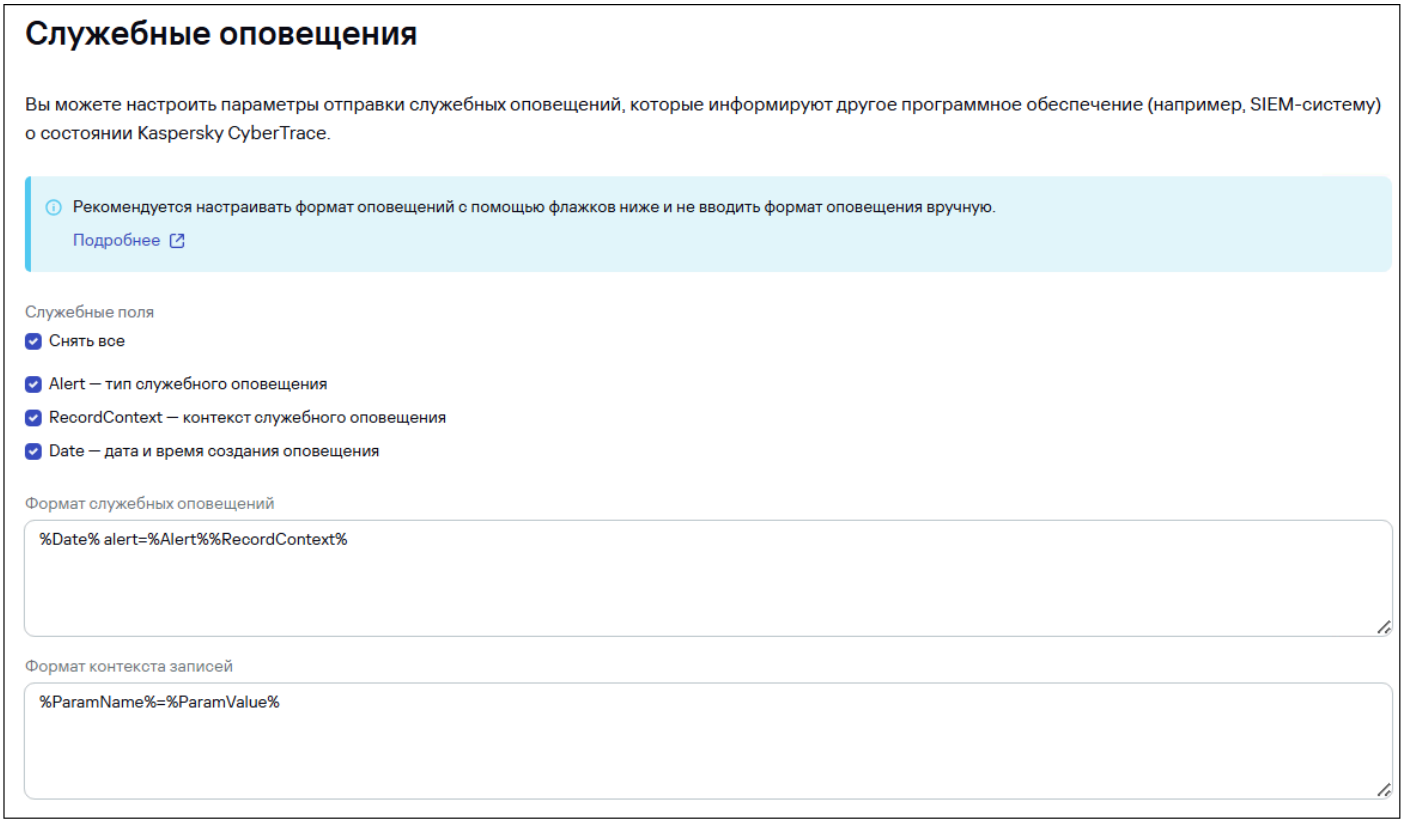
  Сброс всей статистики на информационной панели.

  Рекомендуется выполнить эту операцию после успешной интеграции Kaspersky CyberTrace с SIEM-системой. Это означает, что на информационной панели не будут отображаться оповещения об обнаружении индикаторов компрометации, сгенерированные во время проверки работоспособности, а будут отображаться только реальные оповещения об обнаружении индикаторов компрометации, если таковые имеются.

Настройка служебных оповещений

Служебные оповещения представляют собой исходящие сообщения, информирующие целевое программное обеспечение (например SIEM-систему) о статусе службы Kaspersky CyberTrace.

Настройка служебных оповещений выполняется в веб-интерфейсе Kaspersky CyberTrace на странице **Параметры → Служебные оповещения**. Для работы с этим разделом необходимо перейти в режим Управление системой. Этот режим доступен только пользователям с ролью «Администратор».



Страница **Параметры → Служебные оповещения**

На странице **Служебные оповещения** можно задать форматы служебных оповещений и контекст записи.

Изменять формат оповещений вручную не рекомендуется. Вместо этого установите флажки для шаблонов, которые требуется использовать в оповещениях, после чего Kaspersky CyberTrace автоматически обновит формат.

На этой странице имеются следующие поля ввода:

- **Формат служебных оповещений** — укажите формат исходящих оповещений.
- **Формат контекста записей** — укажите формат, в котором имена и значения полей потока данных вставляются в исходящие оповещения.

Настройка форматов событий и оповещений для определенных SIEM-систем

Правильный формат оповещений о событиях и оповещениях об обнаружении индикаторов компрометации зависит от используемой SIEM-системы. В случае изменения формата событий или оповещений в Kaspersky CyberTrace также может потребоваться перенастройка интеграции с SIEM-системой.

- В случае ArcSight, возможно, потребуется обновить форматы событий и поля контекста.
- В случае QRadar, возможно, потребуется добавить парсинг новых полей.

- В случае RSA NetWitness, возможно, потребуется указать способ парсинга новых полей (см. также раздел Устранение неполадок RSA NetWitness).
- В случае LogRhythm, возможно, потребуется задать способ парсинга новых полей.

О шаблонах формата служебных оповещений

Форматы и шаблоны позволяют включать определенную информацию в служебные оповещения, генерируемые Kaspersky CyberTrace.

Форматы — это строки, определяющие формат оповещения или шаблона. *Шаблоны* — это специальные подстановочные строки, которые можно использовать при определении форматов. При генерации оповещения шаблон заменяется фактическими данными.

Формат контекста записи

Формат *%RecordContext%* определяет, каким образом к оповещению должны добавляться поля контекста. Этот формат можно указать в настройке служебных оповещений.

В формате *%RecordContext%* можно использовать следующие шаблоны:

- *%ParamName%*

  Имя поля в потоке данных.

- *%ParamValue%*

  Значение поля.

Формат *%RecordContext%* определяет формат полей контекста, передаваемых в служебном оповещении.

У каждого типа служебного оповещения особые поля. Например, если для *%RecordContext%* задано `%ParamName%=%ParamValue%`, то при обновлении потока данных об угрозах может быть получена следующая строка: «`feed=Phishing_URL_Data_Feed.json records=200473`».

Формат служебных оповещений

Этот формат можно указать в настройке служебных оповещений.

В этом формате можно использовать следующие шаблоны:

- *%Alert%*

  Тип служебного оповещения.

- *%RecordContext%*

  Контекст оповещения (см. описание выше в разделе «Формат контекста записи»).

- *%Date%*

  Текущие дата и время в формате `Mon DD HH:MM:SS`.

Ниже приведен пример формата служебных оповещений:

```
%Date% alert=%Alert%%RecordContext%
```

Если генерируется оповещение обновления потока данных об угрозах, в приведенном выше примере будет получено следующее оповещение:

```
Apr 16 09:05:41 alert=KL_ALERT_UpdatedFeed feed=Phishing_URL_Data_Feed.json records=200473
```

Шаблоны для ArcSight

Kaspersky CyberTrace Service отправляет служебные оповещения в формате CEF. Форматы сообщений для ArcSight должны соответствовать требованиям формата CEF.

Используется следующий формат:

```
CEF:0|Kaspersky Lab|Kaspersky CyberTrace for ArcSight|2.0|1|CyberTrace Service Event|4| reason=%Alert%
msg=%RecordContext%
```

В приведенном выше формате `4` (или другое значение от `1` до `10`) — это уровень важности служебного оповещения от Kaspersky CyberTrace.

Шаблоны для RSA NetWitness

Значения форматов служебных оповещений должны соответствовать форматам, заданным в файле v20_cybertracemsg.xml. В случае изменения форматов эти изменения необходимо также перенести в файл v20_cybertracemsg.xml.

Служебные оповещения, отправляемые Kaspersky CyberTrace

В этом разделе приводится описание служебных оповещений, которые может генерировать Kaspersky CyberTrace.

KL_ALERT_ConfigurationUpdated

Это оповещение генерируется, если Kaspersky CyberTrace Service перезагрузил конфигурационный файл.

У этого оповещения нет полей контекста.

KL_ALERT_FeedBecameAvailable

Это оповещение генерируется, если стал доступен поток данных об угрозах, который можно использовать с текущим сертификатом.

У этого оповещения есть следующее поле:

- *feed*

  Имя потока данных об угрозах.

KL_ALERT_FeedBecameUnavailable

Это оповещение генерируется, если стал недоступен поток данных об угрозах, который используется с текущим сертификатом.

У этого оповещения есть следующее поле контекста:

- *feed*

  Имя потока данных об угрозах.

KL_ALERT_OutdatedFeed

Это оповещение генерируется, если поток данных об угрозах не обновлялся в течение заданного периода.

У этого оповещения есть следующее поле контекста:

- *feed*

  Имя потока данных об угрозах.

KL_ALERT_ServiceUnavailable

Это оповещение генерируется, когда модуль мониторинга работоспособности обнаруживает сбой или зависание Kaspersky CyberTrace Service.

У этого оповещения нет полей контекста.

KL_ALERT_ServiceStopped

Это оповещение генерируется при успешной остановке Kaspersky CyberTrace Service.

У этого оповещения нет полей контекста.

KL_ALERT_ServiceStarted

Это оповещение генерируется при успешном запуске Kaspersky CyberTrace Service.

У этого оповещения нет полей контекста.

KL_ALERT_UpdatedFeed

Это оповещение генерируется при обновлении и загрузке потока данных об угрозах в Kaspersky CyberTrace Service. Это означает, что новые индикаторы из потока данных об угрозах можно использовать в процессе сопоставления. Обратите внимание, что индикаторы могут быть добавлены в базу данных позже, поскольку они загружаются асинхронно.

У этого оповещения есть следующие поля контекста:

- *feed*

  Имя потока данных об угрозах.

- *records*

  Количество записей, загруженных из потока данных об угрозах.

KL_ALERT_FailedToUpdateFeed

Это оповещение генерируется, когда Kaspersky CyberTrace Service не удается загрузить новый поток данных об угрозах (например, из-за ограничения на количество индикаторов, налагаемого лицензионным ключом), и продолжает использоваться старый поток данных об угрозах:

У этого оповещения есть следующие поля контекста:

- *feed*

  Имя потока данных об угрозах.

- *error*

  Сообщение об ошибке из Feed Utility или текст «`Error while applying feed <FeedName>`».

KL_ALERT_LicenseExpires

Это оповещение генерируется для информирования о том, что срок действия используемого лицензионного ключа вскоре истечет.

Если лицензионный ключ был добавлен с помощью файла ключа, в оповещении сообщается о том, что срок действия лицензионного ключа истечет менее чем через 30 дней; если лицензионный ключ был добавлен с помощью кода активации, в оповещении сообщается о том, что срок действия лицензионного ключа истечет через 10 дней.

У этого оповещения есть следующие поля контекста:

- *license_name*

  Имя лицензионного ключа.

- *expiration_date*

  Дата окончания срока действия лицензионного ключа.

KL_ALERT_LicenseExpired

Это оповещение генерируется, когда истекает срок действия текущего лицензионного ключа.

У этого оповещения есть следующие поля контекста:

- *license_name*

  Имя лицензионного ключа.

- *expiration_date*

  Дата окончания срока действия лицензионного ключа.

KL_ALERT_EPSLimitExceeded

Оповещение генерируется, когда часовой EPS системы превышает пороговый EPS системы.

Это оповещение отправляется только при использовании лицензионного ключа коммерческой лицензии. Это оповещение не выдается для уровня лицензирования Community Edition.

Оповещение отправляется не чаще одного раза в 60 минут.

После формирования оповещения Kaspersky CyberTrace продолжает принимать и обрабатывать события.

У этого оповещения есть следующие поля контекста:

- *avg_system_eps*

  Средний EPS системы на момент превышения лимита.

- *limit_eps*

  Пороговый EPS системы.

KL_ALERT_EPSHardLimit

Это оповещение генерируется, когда часовой EPS системы превышает пороговый EPS системы в течение более чем 30% времени за последние 7 дней.

После формирования оповещения Kaspersky CyberTrace принимает события, превышающие пороговый EPS системы, но не обрабатывает их.

У этого оповещения есть следующие поля контекста:

- *limit_eps*

  Пороговый EPS системы.

KL_ALERT_LicenseChanged

Это оповещение генерируется, когда Kaspersky CyberTrace начинает использовать другой лицензионный ключ или другой уровень лицензирования.

У этого оповещения есть следующие поля контекста:

- *license_name*

  Имя лицензионного ключа.

- *expiration_date*

  Дата окончания срока действия лицензионного ключа.

KL_ALERT_RetroScanCompleted

Это оповещение генерируется при успешном выполнении задачи ретроспективного сканирования.

У этого оповещения есть следующие поля контекста:

- *iocs_rescanned*

  Количество проверенных индикаторов.

- *iocs_detected*

  Количество обнаруженных индикаторов.

- *retroscan_report*

  Ссылка на результат ретроспективного сканирования.

  Это поле отсутствует, если значение поля *iocs_detected* равно 0.

KL_ALERT_RetroScanError

Это оповещение генерируется при отказе задачи ретроспективного сканирования.

У этого оповещения есть следующее поле контекста:

- *error*

  Краткое текстовое описание ошибки.

KL_ALERT_RetroScanStorageExceeded

Это оповещение генерируется при превышении ограничения на размер сохраняемых событий.

У этого оповещения есть следующее поле контекста:

- *storage_size_limit*

  Ограничение на размер сохраняемых событий в мегабайтах.

KL_ALERT_FreeSpaceEnds

Это оповещение генерируется, когда на диске остается мало свободного места.

У этого оповещения есть следующее поле контекста:

- *msg*

  Объем дискового пространства, доступного для базы данных индикаторов на текущий момент.

  Оповещение имеет следующий формат: «Free space left: %FreeSpace% Mb», где %FreeSpace% — остающееся свободным пространство для базы данных индикаторов в МБ.

KL_ALERT_IndicatorsStoreLimitExceeded

Это оповещение генерируется при превышении ограничения на размер сохраняемых индикаторов.

У этого оповещения есть следующие поля контекста:

- *current_indicators_count*

  Текущее количество индикаторов.

- *license_limit_indicators*

  Ограничение на количество индикаторов, налагаемое лицензионным ключом.

KL_ALERT_DetectsStorageExceeded

Это оповещение генерируется при превышении ограничения на размер сохраняемых оповещений об обнаружении индикаторов компрометации.

У этого оповещения есть следующее поле контекста:

- *storage_size_limit*

  Ограничение на размер сохраняемых оповещений об обнаружении индикаторов компрометации в мегабайтах.

KL_ALERT_IndicatorsStoreHardLimit

Это оповещение генерируется, когда Kaspersky CyberTrace ограничивает добавление и обновление индикаторов.

У этого оповещения есть следующие поля контекста:

- *license_limit_indicators*

  Ограничение на количество индикаторов, налагаемое лицензионным ключом.

- *msg*

  Оповещение о том, что новые индикаторы не могут быть добавлены в базу данных из-за ограничения на количество индикаторов, налагаемого лицензионным ключом.

KL_ALERT_FeedEnabled

Это оповещение генерируется при включении потока данных в тенанте.

У этого оповещения есть следующее поле контекста:

- *feed*

  Имя потока данных об угрозах.

KL_ALERT_FeedDisabled

Это оповещение генерируется при отключении потока данных, использовавшегося в тенанте.

У этого оповещения есть следующее поле контекста:

- *feed*

  Имя потока данных об угрозах.

KL_ALERT_FailedToCheckLicense

Это оповещение генерируется, если Kaspersky CyberTrace не может обновить информацию о лицензионном ключе, добавленном с помощью кода активации.

У этого оповещения есть следующие поля контекста:

- *license_name*

  Уровень лицензирования.

- *expiration_date*

  Истечение срока действия лицензионного ключа.

KL_ALERT_AuditPermissionApplyFailed

Это оповещение генерируется, когда Kaspersky CyberTrace не удается применить права доступа к каталогу или файлам журнала аудита действий пользователей.

У этого оповещения есть следующие поля контекста:

- *file_path*

  Полный путь к каталогу или файлу, содержащему журнал аудита действий пользователей, к которому Kaspersky CyberTrace не удалось применить права доступа.

- *error*

  Описание ошибки.

KL_ALERT_AuditWriteFailed

Это оповещение генерируется, когда Kaspersky CyberTrace не удается записать событие в журнал аудита действий пользователей. Генерация этого оповещения возможна не чаще, чем раз в 10 минут.

У этого оповещения есть следующие поля контекста:

- *file_path*

  Полный путь к файлу журнала аудита действий пользователей, в который Kaspersky CyberTrace не удалось записать событие действия пользователя.

- *error*

  Описание ошибки.

- *failed_events_count*

  Общее количество неуспешных попыток записать данное событие действия пользователя за 10 минут, предшествовавшие генерации оповещения.

KL_ALERT_AuditSendingFailed

Это оповещение генерируется, когда Kaspersky CyberTrace не удается отправить событие действия пользователя в какое-либо программное обеспечение по протоколу TCP. Генерация этого оповещения возможна не чаще, чем раз в 10 минут.

У этого оповещения есть следующие поля контекста:

- *address*

  IP-адрес или имя хоста с портом, по которым Kaspersky CyberTrace не удалось отправить событие действия пользователя.

- *error*

  Описание ошибки.

- *failed_events_count*

  Общее количество неуспешных попыток отправить данное событие действия пользователя за 10 минут, предшествовавшие генерации оповещения.

Пользовательские настройки

Для настройки учетных записей пользователей используется страница **Параметры** → **Пользователи**. Для работы с этим разделом необходимо перейти в режим **Управление системой**. Этот режим доступен только пользователям с ролью «Администратор».

Из-за ограничений, налагаемых уровнем лицензирования, эта функция может быть отключена.

Страница **Пользователи** содержит следующие вкладки:

- **Локальные пользователи**

  На этой вкладке можно добавить новую учетную запись пользователя, а также изменить или удалить существующие учетные записи пользователей.

- **Пользователи LDAP**

  На этой вкладке можно настроить порядок использования доменных учетных записей пользователей для аутентификации в веб-интерфейсе Kaspersky CyberTrace.

Настройка пользовательского сеанса

Вы можете настроить допустимое время бездействия пользователя, нажав на кнопку **"Настройки пользовательского сеанса"**.

Пользовательский сеанс в CyberTrace длится недолго, но CyberTrace постоянно обновляет его, пока пользователь активен.

Вы можете указать, в течение какого срока CyberTrace будет обновлять ваш сеанс, когда вы не активны.

Чтобы настроить время бездействия пользователя:

1. Нажмите на кнопку **"Настройки пользовательского сеанса"**.
2. На боковой панели **"Настройки пользовательского сеанса"** выберите одну из следующих вкладок в разделе **"Продлевать сеанс при отсутствии активности"**:

   - **Как можно дольше**

     Этот элемент отключен по умолчанию.

   - **Несколько минут**

     При выборе этого элемента укажите временной период в поле **"Количество минут"**. Вы можете ввести значение от 1 до 480 минут.

     Если элемент **"Как можно дольше"** отключен, по умолчанию промежуток до выхода из системы составляет 480 минут.

3. Нажмите на кнопку **Save**.

После этого настройка времени бездействия пользователя будет завершена.

Продолжительность вашего сеанса также может зависеть от используемого вами браузера. Если браузер (особенно это касается Chrome) переводит окно в "замороженное" состояние, сеанс не будет продлеваться. При этом браузер останавливает все процессы на вкладке. Это может произойти в следующих случаях:

- Операционная система была заблокирована.
- Вкладка долгое время была неактивна, и системе не хватает ресурсов (процессору или оперативной памяти требуется больше свободного места).
- Вкладка не отображается или долгое время не использовалась.
- При использовании режима энергосбережения браузер начинает активнее "замораживать" процессы вкладок.

Работа с локальными учетными записями

Kaspersky CyberTrace поддерживает многопользовательский режим. На вкладке **Локальные пользователи** страницы **Параметры** → **Пользователи** можно добавить новую учетную запись пользователя, а также изменить или удалить существующие учетные записи пользователей.

Форма управления настройками учетных записей пользователей может быть недоступна из-за ограничений, налагаемых уровнем лицензирования. В этом случае будет доступна только учетная запись `admin`.

Чтобы добавить новую учетную запись, выполните следующие действия:

1. Нажмите на кнопку **Добавление пользователя**.

   Откроется окно **Добавление пользователя**.

2. Введите имя учетной записи пользователя в поле **Имя пользователя**.

   > Если параллельно с локальными учетными записями используется доменная аутентификация, не создавайте локальные учетные записи с именами, которые уже используются для доменных учетных записей.

3. Введите полное имя в поле **Полное имя**.

   Это поле можно не заполнять.

4. Задайте пароль пользователя в поле **Пароль** и введите его еще раз в поле **Подтвердите пароль**.

   Пароль должен содержать от 6 до 30 символов ASCII: в нем должна быть хотя бы одна большая латинская буква, одна маленькая латинская буква, одна цифра и один символ другого типа (например, запятая, восклицательный знак или знак №).

5. Выберите роль пользователя:

   - **Администратор**. Администраторы могут управлять учетными записями пользователей и настраивать Kaspersky CyberTrace. Они также могут пользоваться всеми возможностями Kaspersky CyberTrace для мониторинга и создания отчетов.

   - **Менеджер тенанта**. Менеджеры тенантов могут настраивать тенанты, к которым у них есть доступ. Они также могут работать с мониторингом и отчетами в рамках своих тенантов.

   - **Аналитик**. Аналитики могут работать с мониторингом и отчетами в рамках тенантов, к которым у них есть доступ.

   Если выбрана роль **Менеджер тенанта** или **Аналитик**, выберите тенанты, к которым у пользователя должен быть доступ: либо конкретные существующие тенанты, либо все тенанты, включая тех, которые будут добавлены в будущем.

   > При отключенном режиме мультитенантности из-за ограничений, налагаемых уровнем лицензирования, назначить роль **Менеджер тенанта** и выбрать тенанты невозможно.

   По умолчанию назначается роль **Администратор**.

6. Чтобы создать учетную запись, нажмите **Добавить**.

Добавленная учетная запись пользователя отображается в списке учетных записей.

Чтобы изменить учетную запись пользователя, выполните следующие действия:

1. Нажмите на кнопку (**Изменить**) рядом с учетной записью пользователя, которую требуется изменить.

   Откроется окно **Переключение пользователей**.

2. Отредактируйте обязательные поля.

   > Вы не можете изменить роль своей учетной записи.

3. Нажмите на кнопку **Сохранить**.

Учетная запись пользователя обновляется в списке учетных записей.

Чтобы удалить учетную запись пользователя, выполните следующие действия:

1. Нажмите на кнопку (**Удалить**) рядом с учетной записью пользователя, которую требуется удалить.

   > Удалить собственную учетную запись невозможно.

2. В открывшемся окне подтверждения **Удалить пользователя?** нажмите на кнопку **Удалить**, чтобы подтвердить удаление выбранной учетной записи.

Учетная запись пользователя удаляется из списка учетных записей.

Настройка аутентификации LDAP

Kaspersky CyberTrace поддерживает аутентификацию пользователей LDAP, что обеспечивает возможность аутентификации пользователя в веб-интерфейсе Kaspersky CyberTrace под доменной учетной записью. В этом разделе описывается порядок настройки данного типа аутентификации. Сведения о параметрах подключения LDAP см. в справке по настройке.

Kaspersky CyberTrace поддерживает использование Active Directory® только в том случае, если контроллер домена работает под управлением Windows. Использование Active Directory с контроллерами домена на базе Linux возможно, но не гарантируется.

Корневой сертификат сервера Active Directory должен находиться в системном хранилище операционной системы, в которой установлено приложение Kaspersky CyberTrace.

Вкладка **Пользователи LDAP** страницы **Параметры** → **Пользователи** позволяет выполнять следующие действия:

- Включение аутентификации LDAP
- Настройка подключения
- Тестирование соединения с сервером LDAP
- Настройка фильтрации учетных записей

Включение аутентификации LDAP

Чтобы включить аутентификацию LDAP, выполните следующие действия:

1. Нажмите на кнопку **Настроить LDAP**.
2. В открывшемся окне **Настроить LDAP** включите переключатель **Включено**.

В результате сервер LDAP будет использоваться для аутентификации пользователей.

При включенной аутентификации LDAP с Kaspersky CyberTrace можно работать и под учетной записью локального пользователя.

Параметры соединения

В разделе **Параметры соединения** на странице **Настроить LDAP** можно указать следующие настройки:

- IP-адрес или полное доменное имя (FQDN) и порт сервера LDAP.

  Используйте порты глобального каталога для подключения к серверу LDAP: порт 3268 для StartTLS, а также для подключения без шифрования; и порт 3269 для TLS.

- Защита соединения с помощью SSL

В веб-интерфейсе Kaspersky CyberTrace можно включить использование защищенного соединения с сервером LDAP выбрав SSL/TLS или STARTTLS. По умолчанию выбран протокол SSL/TLS.

В Linux при подключении к серверу LDAP Kaspersky CyberTrace проверяет сертификаты.

Каталог с сертификатами `/etc/ssl/certs` содержит символическую ссылку на корневой сертификат. Имя ссылки содержит хеш сертификата. Также каталог обязательно должен содержать символические ссылки на все сертификаты. В противном случае соединение не будет включено, даже если цепочка сертификатов доступна в каталоге `/etc/ssl/certs`.

При работе на Linux deb формат имени сертификата задается утилитой `update-ca-certificates`.

При работе на Linux rpm формат имени сертификата задается пользователем вручную с помощью команды `openssl x509 -in YOUR_CERT_FILE -hash –noout`.

Если включено безопасное соединение, Kaspersky CyberTrace использует для аутентификации сервера LDAP сертификаты из каталога `/etc/ssl/certs`.

- Путь к базе данных LDAP

  Путь к базе данных, содержащей учетные записи пользователей, которым разрешен доступ к Kaspersky CyberTrace.

  Значение должно начинаться с `dc=`.

Тестирование соединения с сервером LDAP

Выполните действия в описанном ниже порядке, чтобы убедиться, что соединение с сервером LDAP установлено.

Чтобы протестировать соединение с сервером LDAP, выполните следующие действия:

1. Нажмите на кнопку **Проверка соединения**.

   Откроется окно **Проверка соединения с LDAP**.

2. Задайте следующие настройки:

   - Имя пользователя для тестового соединения
   - Пароль пользователя для тестового соединения

3. Нажмите на кнопку **Проверить**.

Проверить соединение можно только в том случае, если указаны все необходимые настройки для подключения к серверу.

Фильтрация учетных записей

Раздел **Фильтрация учетных записей** содержит правила фильтрации учетных записей администраторов и аналитиков.

Настроить можно следующие свойства:

- **Формат учетной записи**

Можно выбрать один из двух форматов:

- **UPN-имя (user)**

  Если выбран этот вариант, при выполнении аутентификации пользователи должны предоставить имя пользователя, которое не является адресом электронной почты (например, *user*, но не *user@domain.com*).

- **Имя учетной записи sAM (Domain\\User)**

  Если выбран этот вариант, при выполнении аутентификации пользователи должны предоставить имя пользователя в следующем формате: *Domain**User*.

- **Фильтр для администраторов**

  Фильтр для учетных записей пользователей LDAP, определяющий, каким пользователям должна быть назначена роль «Администратор» в зависимости от их *общего имени* в Active Directory.

  Если это значение не задано, пользователи не могут осуществлять вход посредством аутентификации LDAP и получать роль «Администратор».

- **Фильтр для аналитиков**

  Фильтр для учетных записей пользователей LDAP, определяющий, каким пользователям должна быть назначена роль «Аналитик» в зависимости от их *общего имени* в Active Directory.

  Если это значение не задано, пользователи не могут осуществлять вход посредством аутентификации LDAP и получать роль «Аналитик».

  Например, на рисунке ниже фильтры настроены таким образом, что пользователям, входящим в группу `Admins`, будет назначаться роль «Administrator», а пользователям, входящим в группу `Operators` или `Analysts`, будет назначаться роль «Analyst».



Пример фильтров учетных записей

Если элементы `AdministratorAccountsFilter` и `AnalystAccountsFilter` файла kl_feed_service.conf содержат значения, а пользователь, пытающийся войти в систему, не входит ни в одну из указанных групп, Kaspersky CyberTrace вернет ошибку и запретит доступ к веб-интерфейсу для этого пользователя.

Фильтрация учетных записей для тенантов

Раздел **Фильтрация учетных записей для тенантов** содержит правила фильтрации учетных записей менеджеров тенантов и аналитиков для тенантов, добавленных в Kaspersky CyberTrace.

Для каждого тенанта можно настроить следующие свойства:

- **Фильтр для менеджеров тенанта**

  Фильтр для учетных записей пользователей LDAP, определяющий, каким пользователям должна быть назначена роль «Менеджер тенанта» в зависимости от их *общего имени* в Active Directory.

  Если значение не указано, в данном тенанте ни один пользователь не имеет этой роли.

- **Фильтр для аналитиков**

  Фильтр для учетных записей пользователей LDAP, определяющий, каким пользователям должна быть назначена роль «Аналитик» в зависимости от их *общего имени* в Active Directory.

  Если значение не указано, в данном тенанте ни один пользователь не имеет этой роли.

Настройка тенантов

Kaspersky CyberTrace поддерживает мультитенантную архитектуру, позволяющую управлять тенантами. Тенант — это специфичный для клиента набор параметров конфигурации. Тенанты особенно подходят провайдерам услуг безопасности (MSSP), позволяя дифференцированно работать с клиентами в рамках единого экземпляра Kaspersky CyberTrace.

Из-за ограничений, налагаемых уровнем лицензирования, эта функция может быть отключена.

Kaspersky CyberTrace использует тенант «General», который позволяет задавать общие настройки. Для создания или изменения тенантов в веб-интерфейсе Kaspersky CyberTrace используется раздел **Параметры** → **Тенанты**. Для работы с этим разделом необходимо перейти в режим **Управление системой**. Этот режим доступен только пользователям с ролью «Администратор».

В разделе **Тенанты** можно просматривать следующие значения EPS (событий в секунду) и IPS (индикаторов в секунду) для тенантов, используемых в Kaspersky CyberTrace:

- **Сумма пороговых EPS тенантов**
- **Пороговый EPS системы**
- **Средний TCP EPS**
- **Средний API IPS**
- **Пороговый TCP EPS**

Также доступны следующие действия:

- Добавление нового тенанта
- Переход к настройке тенанта
- Удаление тенанта

Из раздела **Тенанты** можно перейти в разделы **Потоки данных**, **Источники событий**, **Служебные оповещения** и **Обнаружения** и задать параметры для тенанта.

При настройке тенанта необходимо также выбрать SIEM-систему, с которой необходимо интегрировать данный тенант. В Kaspersky CyberTrace для каждой SIEM-системы используется ряд предустановленных параметров, таких как параметры парсинга событий и формата событий (для оповещений об обнаружении киберугроз и служебных оповещениях).

Поддерживаются следующие SIEM-системы:

- Kaspersky Unified Monitoring and Analysis Platform
- Splunk
- ArcSight
- QRadar
- RSA NetWitness
- LogRhythm

Добавление тенанта

Чтобы добавить тенант, выполните следующие действия:

1. Нажмите на кнопку **Добавить тенант**.

   Откроется окно **Добавить тенант**.

2. Введите имя нового тенанта в поле **Имя тенанта**.

   Длина имени тенанта должна составлять от 1 до 64 символов. Допускаются латинские буквы, цифры, специальные символы (" ', . @ # $ % & * № / \) и пробелы.

   > Изменить имя тенанта «General» невозможно.

3. Введите описание этого тенанта в поле **Описание**.

   Длина описания тенанта должна составлять от 0 до 2048 символов. Допускаются латинские буквы, цифры, специальные символы (" ', . @ # $ % & * № / \), пробелы и переносы строки.

4. Выберите SIEM-систему, с которой требуется интегрировать тенант.

   Можно выбрать SIEM-систему, поддерживаемую Kaspersky CyberTrace, или пользовательскую (не поддерживаемую SIEM-систему).

   Эта SIEM-система будет использоваться в рамках данного тенанта для отправки событий в Kaspersky CyberTrace.

   В зависимости от выбранной SIEM-системы Kaspersky CyberTrace определяет наборы регулярных выражений, форматы сообщений об обнаруженных киберугрозах и форматы служебных оповещений, используемых при интеграции с этой SIEM-системой.

5. В разделе **Пороговый EPS тенанта** настройте пороговый EPS тенанта (число событий в секунду — events per second):

   a. Включите переключатель.

   b. В поле **Пороговый EPS** введите требуемое значение порогового EPS.

Если значение EPS приближается к пороговому значению, в веб-интерфейсе отображается предупреждение и генерируется оповещение с предупреждением. При превышении лимита в рамках тенанта сверхлимитный трафик для этого тенанта сбрасывается, отображается предупреждение и генерируется оповещение с предупреждением. Если пороговый EPS тенанта не задан, это может повлиять на другие тенанты (если таковые имеются).

6. В разделе **Входящие события** задайте параметры сокета данного тенанта, который Kaspersky CyberTrace должен прослушивать в ожидании входящих событий:

   a. Выберите тип соединения, который требуется использовать: **IP-адрес и порт** или **Сокет UNIX**.

   b. В зависимости от типа подключения выполните одно из следующих действий:

   - Укажите IP-адрес и порт в полях **IP-адрес** и **Порт**.
   - В поле **Сокет UNIX** укажите сокет UNIX.

   c. Если выбран тип соединения **IP-адрес и порт**, в поле **Защищенное соединение** выберите тип соединения: **TLS** или **Нет**.

7. В блоке **Оповещения об обнаружении индикаторов компрометации** укажите следующие параметры:

   a. В полях **IP-адрес или имя хоста** и **Порт** укажите IP-адрес и порт для конкретного тенанта, которые Kaspersky CyberTrace будет использовать для исходящих оповещений об обнаружении индикаторов компрометации.

   b. В поле **Secure connection** выберите тип соединения: **TLS с проверкой сертификата**, **TLS без проверки сертификата** или **Нет**.

8. Нажмите на кнопку **Сохранить**.

Созданный тенант добавляется в список тенантов.

Изменение тенанта

После создания тенанта можно изменять его параметры, в том числе те параметры, которые не были заданы при создании.

Чтобы изменить тенант, выполните следующие действия:

Рядом с тенантом, который требуется изменить, нажмите **Настроить**, затем выберите соответствующий пункт меню:

- **Общие**

  На открывшейся странице **Параметры** → **Общие** в режиме **Управление данными** можно настраивать общие параметры тенанта.

- **Потоки данных**

  На открывшейся странице **Параметры** → **Потоки данных** в режиме **Управление данными** можно изменить список потоков данных, к которым имеет доступ тенант.

- **Источники событий**

  На открывшейся странице **Параметры** → **Источники событий** в режиме **Управление данными** можно изменить источники события, к которым имеет доступ тенант.

- **Служебные оповещения**

  На открывшейся странице **Параметры** → **Служебные оповещения** в режиме **Управление данными** можно изменить настройки служебных оповещений, снабжающих другое ПО (например, SIEM-систему) информацией о состоянии тенанта.

- **Обнаружения**

  На открывшейся странице **Параметры** → **Обнаружения** в режиме **Управление данными** можно изменить настройки хранения оповещений об обнаружениях индикаторов компрометации в целях дальнейшего анализа и расследования.

Удаление тенанта

Удалить тенант «General» невозможно.

Чтобы удалить тенант, выполните следующие действия:

1. В списке тенантов нажмите на кнопку (**Удалить**) рядом с тенантом, который требуется удалить.
2. В открывшемся окне подтверждения нажмите кнопку **Удалить**.

   Удаленный тенант убирается из списка тенантов.

Настройка потока данных

Управлять параметрами потоков данных можно в веб-интерфейсе Kaspersky CyberTrace на странице **Параметры** → **Потоки данных**. Для работы с этим разделом необходимо перейти в режим **Управление системой**. Этот режим доступен только пользователям с ролью «Администратор».

При изменении настроек предлагается обновить потоки данных об угрозах.

Режим Управление системой позволяет:

- Импорт сертификата для Kaspersky Threat Data Feeds
- Указание периода обновления потоков данных об угрозах
- Включение и отключение потоков данных об угрозах
- Выбор доступных полей для потока данных об угрозах
- Указание правил фильтрации для потока данных об угрозах
- Сокращение потока данных об угрозах
- Указание срока хранения записей потока данных об угрозах

- Запуск обновления потоков данных об угрозах вручную
- Добавление пользовательских или сторонних потоков данных об угрозах
- Настройка пользовательского или стороннего потока данных об угрозах

Вкладки потоков данных об угрозах

Потоки данных об угрозах перечислены на следующих вкладках:

- **Лаборатория Касперского**

  На этой вкладке расположены потоки данных об угрозах Kaspersky Threat Data Feeds.

- *<Название поставщика>*

  Пользовательские и сторонние потоки данных об угрозах сгруппированы на вкладках по поставщикам.

  Если для потока данных не указано имя поставщика, оно отображается на вкладке **Пользовательские потоки данных**.

  Если пользовательские и сторонние потоки данных об угрозах отсутствуют, эти вкладки не отображаются.

- **OSINT**

  На этой вкладке расположены потоки данных об угрозах OSINT.

- **Пользовательский список индикаторов**

  На этой вкладке расположен источник данных об угрозах **Пользовательский список индикаторов**, содержащий индикаторы, добавленные в базу данных пользователями.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы) может быть недоступна в программе на территории США.

О потоках данных «Лаборатории Касперского», пользовательских и сторонних потоках данных

В этом разделе описаны потоки данных об угрозах, доступные в Kaspersky CyberTrace.

О потоках данных об угрозах «Лаборатории Касперского»

Для Kaspersky CyberTrace предоставляются потоки данных об угрозах Kaspersky Threat Data Feeds. В Kaspersky CyberTrace естественным образом интегрированы потоки данных об угрозах Kaspersky Threat Data Feeds, которые предоставляют тщательно отобранные данные индикаторов угроз.

О пользовательских и сторонних потоках данных об угрозах

Пользовательские и сторонние потоки данных об угрозах — это потоки данных об угрозах, которые можете добавлять в Kaspersky CyberTrace.

Добавление или удаление сторонних потоков данных об угрозах или включение использования потоков данных об угрозах OSINT может быть отключено из-за ограничений, налагаемых уровнем лицензирования. В этом случае форма добавления пользовательского или стороннего потока данных может быть отключена.

Кодировка пользовательских и сторонних сторонний потоков данных об угрозах

Все пользовательские или сторонние потоки данных об угрозах, добавляемые в Kaspersky CyberTrace, должны быть в кодировке UTF-8. Если пользовательские или сторонние потоки данных об угрозах имеют другую кодировку, их необходимо конвертировать в UTF-8. Можно добавлять пользовательские потоки данных, содержащие маски подсетей для сетей класса C. Эти потоки данных об угрозах можно использовать в процессе сопоставления, отметив поле потока данных об угрозах как «IP».

Сертификаты и демонстрационные потоки данных

Kaspersky CyberTrace загружает и обновляет Потоки данных «Лаборатории Касперского» об угрозах, доступные с текущим сертификатом. С сертификатом по умолчанию доступны только демонстрационные потоки данных об угрозах.

Если используются демонстрационные потоки данных об угрозах, при выборе вкладки **Параметры → Потоки данных** выводится уведомление. В этом уведомлении сообщается что используются демонстрационные потоки данных об угрозах «Лаборатории Касперского», а также приводится информация о том, как приобрести коммерческие потоки данных об угрозах, обеспечивающие более высокий уровень защиты. Ссылка в уведомлении ведет на форму Запрос на доступ к решениям портала Kaspersky Threat Intelligence, которая позволяет подписаться на Kaspersky Threat Intelligence Portal и получить доступ к коммерческим потокам данных об угрозах.

Импорт сертификата для Kaspersky Threat Data Feeds

В этом разделе описывается порядок импорта сертификата для потоков данных «Лаборатории Касперского» об угрозах.

О сертификате потоков данных об угрозах

Kaspersky CyberTrace загружает и обновляет потоки данных об угрозах Kaspersky Threat Data Feeds, если они доступны, с текущим сертификатом.

Импорт сертификата для потоков данных об угрозах Kaspersky Threat Data Feeds

Чтобы импортировать новый сертификат для потоков данных об угрозах Kaspersky Threat Data Feeds, выполните следующие действия:

1. Перейдите на страницу **Параметры → Потоки данных**.
2. Под разделом обновления потоков данных нажмите на кнопку **Импортировать сертификат**.

   Откроется окно **Импортировать сертификат**.
3. В окне **Импортировать сертификат** выберите ссылку **Выбрать**.
4. В открывшемся окне браузера выберите файл сертификата в формате .pem и откройте его.
5. В окне **Импортировать сертификат** нажмите кнопку **Сохранить**.

После импорта нового сертификата Kaspersky CyberTrace Service проверит наличие всех потоков данных об угрозах, доступных с этим сертификатом, и отобразит их.

Указание периода обновления потоков данных об угрозах по умолчанию

В этом разделе описывается период обновления потоков данных по умолчанию.

О периоде обновления потоков данных об угрозах по умолчанию

Период обновления потоков данных об угрозах по умолчанию определяет, как часто Kaspersky CyberTrace обновляет все включенные потоки данных об угрозах. Период обновления потоков данных по умолчанию составляет 30 минут. Отображается дата и время последнего обновления потоков данных об угрозах.

В случае источников данных об угрозах *FalsePositive* и *InternalTI* и потоков данных, добавленных через общедоступные API, обновление по расписанию невозможно.

Потоки данных об угрозах можно откатить после обновления, если Kaspersky CyberTrace не сможет загрузить новые индикаторы в Matching engine (подробные сведения приведены в описании параметра *FeedsRollbackEnabled* в ServiceSettings).

Также вы можете обновить потоки данных вручную и настроить индивидуальное расписание обновлений для пользовательских потоков данных и OSINT feed.

Использование прокси-сервера для обновления потоков данных

В этом разделе описывается, как использовать прокси-сервер для обновления потоков данных.

Включение и отключение прокси-сервера для потоков данных

Прежде чем включать прокси-сервер для потоков данных, активируйте глобальную настройку прокси-сервера в разделе **"Система"** → **"Настройки"** → **"Служба"** → **"Прокси"**.

Чтобы включить прокси-сервер для потоков данных для решений «Лаборатории Касперского»:

1. Перейдите на страницу **Settings** → **Feeds**.
2. Выберите вкладку **"Kaspersky"**.
3. Включите переключатель **"Прокси-сервер включен"**.

   После этого прокси-сервер будет включен для потоков данных для решений «Лаборатории Касперского».

Чтобы включить прокси-сервер для OSINT и пользовательских потоков данных:

1. Перейдите на страницу **Settings** → **Feeds**.
2. Выберите вкладку с **OSINT** или пользовательским потоком данных.
3. С помощью переключателя включите прокси-сервер для каждого потока данных в окне редактирования потока данных.

   После этого прокси-сервер будет включен для OSINT и пользовательских потоков данных.

Если для потоков данных включен прокси-сервер, в столбце **"Дополнительная информация"** в таблице потоков данных будет отображаться специальный тег.

Если глобальная настройка прокси-сервера отключена, переключатели для включения прокси-сервера будут находиться в режиме только для чтения.

Если поток данных добавлен через общедоступный API, переключатель для включения и отключения прокси-сервера будет недоступен в окне редактирования потока данных.

Если при добавлении или редактировании пользовательского потока данных указан путь к локальному файлу, в окнах добавления или редактирования потока данных будет недоступен переключатель для включения и отключения прокси-сервера.

Включение и отключение потоков данных об угрозах

В этом разделе описывается порядок включения и отключения потоков данных об угрозах.

При включении потока данных об угрозах он автоматически добавляется и включается для всех тенантов. При отключении потока данных об угрозах он автоматически удаляется для всех тенантов.

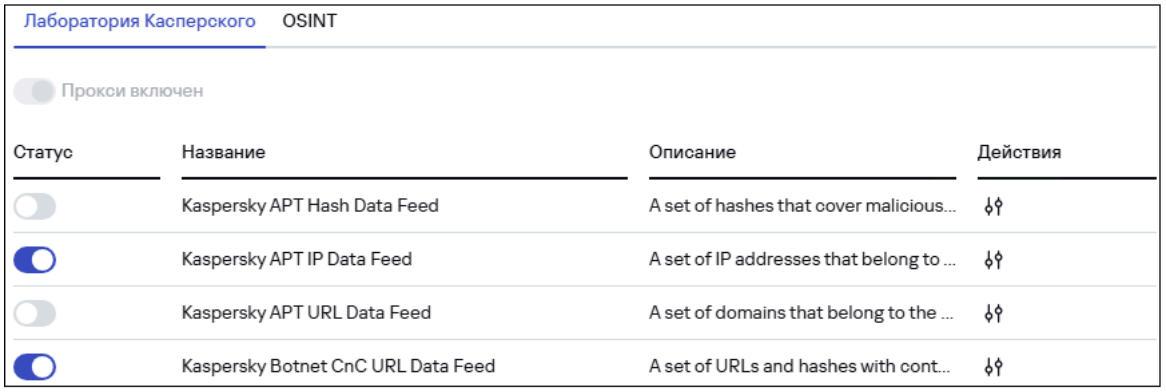
Включение и отключение потоков данных об угрозах

Чтобы включить или отключить потоки данных:

1. Перейдите на страницу **Параметры** → **Потоки данных**.
2. Включите или выключите переключатель в списке потоков данных.

> При отключении потока данных об угрозах его индикаторы не удаляются из базы данных индикаторов. Эти индикаторы не отображаются на странице **Индикаторы**, но учитываются при расчете ограничения на количество индикаторов. Чтобы этого не происходило, индикаторы необходимо удалить вручную перед отключением потока данных об угрозах.

Если используются только демонстрационные потоки данных, можно воспользоваться формой Request Kaspersky Threat Intelligence для подписки на Kaspersky Threat Intelligence Portal и получения коммерческих потоков данных об угрозах, обеспечивающих более высокий уровень защиты.



Включение и отключение потоков данных об угрозах

Выбор доступных полей для потока данных об угрозах

В этом разделе описывается порядок указания полей, которые должны быть включены в поток данных об угрозах.

О доступных полях

Доступные поля для потока данных об угрозах определяют, какие поля из исходного потока данных об угрозах Kaspersky CyberTrace необходимо включить в итоговый поток данных об угрозах. Например, если указать, что игнорироваться должны все поля в потоке данных об угрозах, кроме одного, в итоговом потоке данных об угрозах для каждой записи будет только одно поле.

В потоке данных об угрозах должно быть хотя бы одно доступное поле, которое используется для сопоставления. Это поле должно содержать IP-адреса, хеши или URL.

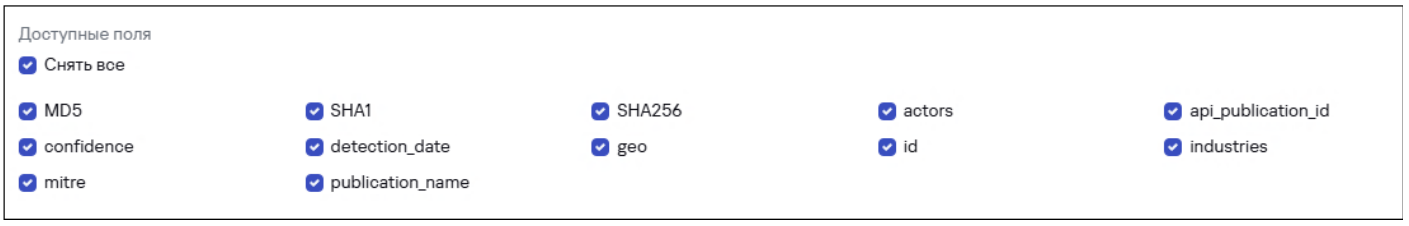
В исходных файлах потоков данных об угрозах некоторые записи могут иметь дополнительные поля или не иметь некоторых полей; у одной записи может быть меньше или больше полей по сравнению с другой записью.

Если у записи есть дополнительное поле и это поле выбрано для включения в поток данных об угрозах, в итоговом потоке данных об угрозах запись будет иметь это поле. Если у записи есть дополнительное поле, и это поле не выбрано для включения в поток данных об угрозах, у записи не будет этого поля в итоговом потоке данных об угрозах.

Если у записи нет поля, и это поле выбрано для включения в поток данных об угрозах, у записи не будет этого поля. Если у записи нет какого-либо поля, и это поле не выбрано для включения в поток данных об угрозах, у записи не будет этого поля.

Если требуется исключить из вывода записи с недостающими полями, необходимо создать правила фильтрации для всех обязательных полей. Для значений полей можно задавать критерии.

Выбор доступных полей для потока данных об угрозах



Выбор доступных полей потока данных

Чтобы выбрать доступные поля для потока данных, выполните следующие действия:

1. Перейдите на страницу **Параметры** → **Потоки данных**.
2. В столбце **Действия** списка потоков данных выберите поток данных, который требуется настроить.

> Для источника данных об угрозах *Пользовательские сведения о киберугрозах* невозможно включать или исключать доступные поля.

3. В разделе потока данных **Доступные поля** выберите поля, которые требуется включить, или снимите выделение с полей, которые требуется исключить.

4. Прокрутите страницу до конца и нажмите кнопку **Сохранить**.

Указание правил фильтрации для потока данных об угрозах

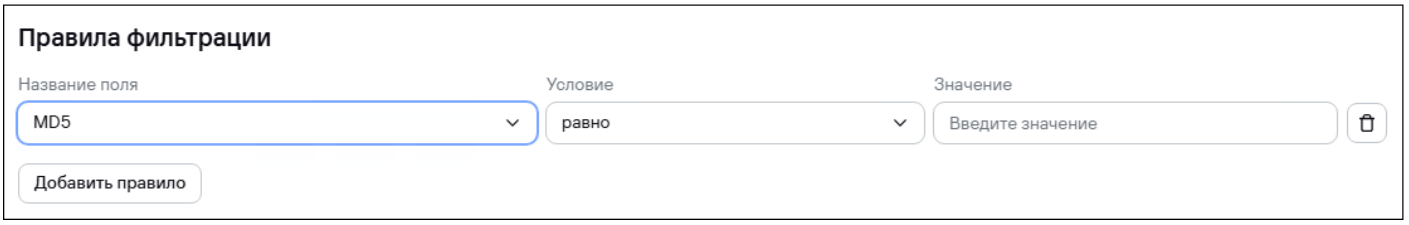
В этом разделе объясняется, что такое правила фильтрации, и описывается порядок их настройки.

О правилах фильтрации

Правила фильтрации представляют собой критерии для потока данных об угрозах, которые позволяют исключать из потока данных об угрозах определенные записи.

Kaspersky CyberTrace использует правила фильтрации для фильтрации загружаемых файлов потоков данных во время обновления. Указанные правила фильтрации применяются к потокам данных после обновления, а не к существующим потокам.

В выходной файл включаются только те записи, которые соответствуют всем указанным критериям. Если для поля указан критерий фильтрации и при этом поле отсутствует в записи, такая запись не будет включена в выходной файл.



Раздел «Filtering rules»

Чтобы указать правило фильтрации для потока данных об угрозах, выполните следующие действия:

1. Перейдите на страницу **Параметры** → **Потоки данных**.

2. В столбце **Действия** списка потоков данных выберите поток данных, который требуется настроить.

   Для источника данных об угрозах *InternalTI* указать правила фильтрации невозможно.

3. В разделе **Правила фильтрации** нажмите на кнопку **Добавить правило**.

4. В раскрывающемся списке **Название поля** выберите имя одного из полей, доступных для потока данных.

   С каждым полем в потоке данных об угрозах может быть связано только одно правило фильтрации. Для одного поля нельзя указать два правила фильтрации.

5. В раскрывающемся списке **Условие** выберите условие фильтрации.

   Список возможных условий фильтрации приведен в разделе «Возможные условия фильтрации» ниже.

6. В поле ввода **Значение** укажите критерий фильтрации для поля.

Для разделения значений в этом поле ввода запрещается использовать точку с запятой («**;**»). Вместо этого выберите **среди перечисленных (разделенные новой строкой)** в раскрывающемся списке **Условие** и используйте символ переноса строк («\n») или нажимайте клавишу **Enter** для разделения значений. В противном случае правило фильтрации не будет применяться правильно.

Дополнительная информация о порядке задания определенных критериев фильтрации приведена в подразделах «Определение критериев фильтрации для числовых значений», «Определение критериев фильтрации для строк» и «Определение критериев фильтрации для дат» в разделе Правила фильтрации.

7. Прокрутите страницу до конца и нажмите кнопку **Сохранить**.

Возможные условия фильтрации

В таблице ниже перечислены условия фильтрации, которые можно применить к потокам данных об угрозах:

Возможные условия фильтрации

Условие фильтрации	Описание
Сопоставление с точным значением	Поле в потоке данных об угрозах в точности соответствует указанному значению. Чтобы применить это условие, выберите **равно** в раскрывающемся списке **Условие**, затем укажите одно значение в поле ввода **Значение**.
Сопоставление хотя бы с одним из нескольких возможных значений	Поле в потоке данных об угрозах должно содержать одно или несколько указанных значений. Чтобы применить это условие, выберите **среди перечисленных (разделенные новой строкой)** в раскрывающемся списке **Условие**, затем укажите несколько значений в поле ввода **Значение**. Не указывайте пустые значения. Каждое следующее значение должно начинаться с новой строки.
Принадлежит к диапазону числовых значений	Поле в потоке данных об угрозах должно содержать значение из указанного диапазона. Чтобы применить это условие, выберите **в диапазоне (включительно)** в раскрывающемся списке **Условие**, затем укажите диапазон значений в полях ввода **Значение**. Обратите внимание, что граничные значения включаются в диапазон. Значения должны быть целыми числами.
Принадлежит к диапазону числовых значений, которые равны или больше указанного значения	Поле в потоке данных об угрозах должно содержать значение, равное указанному значению или превышающее его. Чтобы применить это условие, выберите **больше (включительно)** в раскрывающемся списке **Условие**, а затем укажите одно значение в поле ввода **Значение**. Значение должно быть целым числом.
Принадлежит к диапазону числовых значений, которые равны или меньше указанного значения	Поле в потоке данных об угрозах должно содержать значение, равное или меньшее заданного значения. Чтобы применить это условие, выберите **меньше (включительно)** в раскрывающемся списке **Условие**, а затем укажите одно значение в поле ввода **Значение**. Значение должно быть целым числом.
Принадлежит к диапазону дат	Атрибут индикатора должен содержать дату в указанном диапазоне. Чтобы применить это условие, выберите **дата в диапазоне (включительно) ИЛИ поле отсутствует** в раскрывающемся списке **Условие**, затем укажите диапазон дат в полях ввода **Значение**. Чтобы выбрать диапазон дат, используйте средство выбора дат в календаре. Кроме того, при указании границ диапазона можно выбрать произвольное количество дней или одно из следующих предустановленных значений: • **День** • **Неделя** • **Месяц** • **3 месяца**

Принадлежит к диапазону дат, которые равны или больше указанного значения	Атрибут индикатора должен содержать дату, равную указанному значению или превышающую его. Чтобы применить это условие, выберите **дата больше (включительно) ИЛИ поле отсутствует** в раскрывающемся списке **Условие**, затем укажите дату в поле ввода **Значение**. Чтобы выбрать дату, используйте средство выбора дат в календаре. Кроме того, для границы можно выбрать одно из следующих предустановленных значений: • **1 day ago** • **7 days ago** • **30 days ago**
Принадлежит к диапазону дат, которые равны или меньше указанного значения	Атрибут индикатора должен содержать дату, которая меньше или равна указанному значению. Чтобы применить это условие, выберите **дата меньше (включительно) ИЛИ поле отсутствует** в раскрывающемся списке **Условие**, затем укажите дату в поле ввода **Значение**. Чтобы выбрать дату, используйте средство выбора дат в календаре. Кроме того, для границы можно выбрать одно из следующих предустановленных значений: • **1 day ago** • **7 days ago** • **30 days ago**
Сопоставление с непустым значением	Поле в потоке данных об угрозах должно содержать любое непустое значение. Чтобы применить это условие, выберите **непустое** в раскрывающемся списке **Условие**.

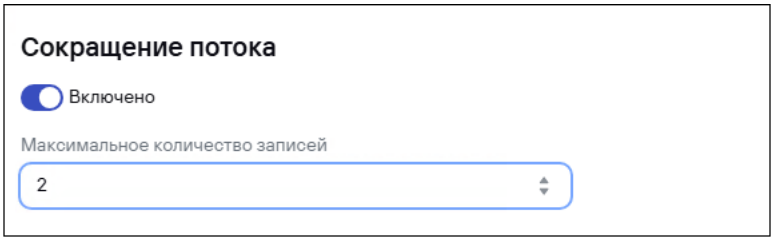
Сокращение потока данных об угрозах

В данном разделе объясняется, как ограничить размер потока данных об угрозах до определенного количества записей.

О максимальном количестве записей в потоке данных об угрозах

По умолчанию Kaspersky CyberTrace импортирует все записи, соответствующие критериям фильтрации потока данных об угрозах. Данное поведение можно изменить, задав максимальное количество записей, подлежащих импорту. Kaspersky CyberTrace импортирует записи в том порядке, в котором они расположены в исходном потоке данных об угрозах, пока не будет достигнуто заданное максимальное количество записей.

Сокращение потока данных об угрозах



Управление количеством записей в потоке данных об угрозах

Чтобы указать максимальное количество записей в потоке данных об угрозах:

1. Перейдите на страницу **Параметры** → **Потоки данных**.
2. В столбце **Действия** списка потоков данных выберите поток данных, который требуется настроить.

> Для источника данных об угрозах *Пользовательские сведения о киберугрозах* задать максимальное количество записей невозможно.

3. В разделе настроек для потока данных включите переключатель **Сокращение потока**.

4. В поле ввода **Максимальное количество записей** укажите максимальное количество записей для потока данных об угрозах.

   Количество записей не может быть меньше 1.

5. Прокрутите страницу до конца и нажмите кнопку **Сохранить**.

Указание срока хранения записей потока данных об угрозах

В этом разделе описывается порядок указания срока хранения индикаторов потока данных, добавленных в базу данных.

Эта настройка применяется к источникам, отличным от потоков данных «Лаборатории Касперского» об угрозах.

Дополнительная информация о сроке хранения приведена в описании атрибута `indicator lifetime` в элементе `Feed` конфигурационного файла.

Указание срока хранения

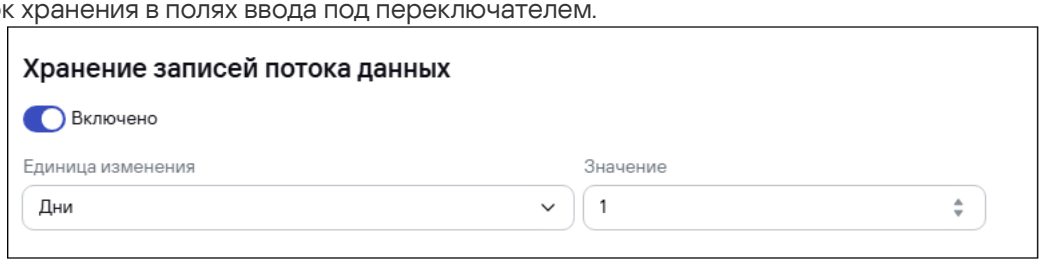
Чтобы указать срок хранения, выполните следующие действия:

1. Перейдите на страницу **Параметры** → **Потоки данных**.

2. В столбце **Действия** списка потоков данных выберите поток данных, который требуется настроить.

3. Включите переключатель в разделе **Хранение записей потока данных**.

4. Задайте срок хранения в полях ввода под переключателем.



Указание срока хранения

5. Прокрутите страницу до конца и нажмите кнопку **Сохранить**.

Запуск обновления потоков данных об угрозах вручную

В этом разделе описывается порядок запуска обновления потока данных об угрозах вручную.

Об обновлении потоков данных об угрозах вручную

Kaspersky CyberTrace обновляет все включенные потоки данных об угрозах автоматически в соответствии с настроенным периодом обновления потоков данных об угрозах. Обновление потоков данных об угрозах также можно в любой момент выполнить вручную.

Если другой пользователь уже запустил обновление, запуск обновления будет невозможен до тех пор, пока потоки данных об угрозах не обновятся.

Запуск обновления потоков данных об угрозах вручную

Чтобы запустить обновление потоков данных об угрозах вручную, выполните следующие действия:

1. Перейдите на страницу **Параметры** → **Потоки данных**.
2. В разделе обновления потоков индикаторов нажмите на кнопку (**Обновить сейчас**).

   В раскрывающемся списке **"Частота обновления по умолчанию"** можно выбрать частоту обновления.

Установка частоты обновления для определенного потока данных

Вы можете установить отдельную частоту обновления для каждого пользовательского потока данных и OSINT feed.

Чтобы настроить частоту обновления для определенного потока данных:

1. Перейдите в раздел **Параметры** → **Потоки данных**.
2. Нажмите **Добавить пользовательский поток данных** или выберите поток данных в таблице.
3. В окне добавления/редактирования потока данных включите переключатель **"Пользовательская частота обновления"**.
4. В раскрывающемся списке выберите значение частоты обновления.

Если задана периодичность обновления по умолчанию, все потоки данных будут обновляться в соответствии с расписанием обновлений потоков данных «Лаборатории Касперского», кроме тех потоков данных, для которых задан индивидуальный период обновления.

При запуске обновления потоков данных вручную также будут обновляться потоки данных, для которых частота обновления указана отдельно.

Для потоков данных, для которых частота обновления указана отдельно, в столбце **"Дополнительная информация"** таблицы потоков данных отображается специальный тег с указанием времени обновления.

Для потоков данных, добавленных через общедоступный API, указание индивидуальной частоты обновления недоступно.

В разделе **Tasks** можно просматривать статусы задачи обновления потоков данных:

- **Выполняется**

  Выполняется обновление потоков данных.

- **Выполнена**

  Все потоки данных успешно скачаны, все индикаторы проверены в Kaspersky CyberTrace.

- **Выполнена (частично)**

  Задача считается частично выполненной, если хотя бы один индикатор хотя бы одного из обработанных потоков данных не прошел проверку в Kaspersky CyberTrace.

- **Ошибка**

  Обновление потока данных не выполнено из-за сбоя при обработке или скачивании потоков данных или при проверке индикаторов.

- **Отменена**

  Задача отменена пользователем.

Если задача обновления потока данных завершилась с ошибкой, на странице **Задачи** для соответствующей задачи будет отображен значок. При наведении курсора на этот значок будет отображена всплывающая подсказка с указанием имен потоков данных, которые не удалось обновить, и причинами ошибок при обновлении.

Добавление пользовательского или стороннего потока данных об угрозах

В этом разделе описывается порядок добавления и настройки пользовательского или стороннего потока данных об угрозах.

> Из-за ограничений, налагаемых уровнем лицензирования, эта функция может быть отключена.

Потоки данных об угрозах можно добавлять только с одним полем типа URL или DOMAIN. Это значит, что если одно поле в потоке данных об угрозах имеет тип URL или DOMAIN, ни одно другое поле в этом потоке данных об угрозах не должно иметь тип URL или DOMAIN. Типы URL и DOMAIN считаются одним и тем же типом поля.

При добавлении поток данных об угрозах автоматически включается для всех тенантов.

> Из-за ограничений, налагаемых уровнем лицензирования, эта функция может быть отключена.

Добавление пользовательского потока данных об угрозах

Чтобы добавить пользовательский поток данных, выполните следующие действия:

1. На странице **Параметры** → **Потоки данных** нажмите **Добавить пользовательский поток данных**.
2. Выберите тип потока данных.

   Тип потока данных об угрозах может быть одним из следующих:

   - **JSON**

     Если поток данных об угрозах в формате JSON содержит поле со значением маски подсети, Kaspersky CyberTrace раскрывает данные только в том случае, если это поле первого уровня. Если это поле вложено, Kaspersky CyberTrace не может раскрыть данные.

     Если потоки данных об угрозах Kaspersky Threat Data Feeds загружаются с ресурса https://wlinfo.kaspersky.com, используется формат JSON. Это значение изменить невозможно.

   - **STIX**

Если поток данных об угрозах имеет формат STIX, также необходимо выбрать версию STIX:

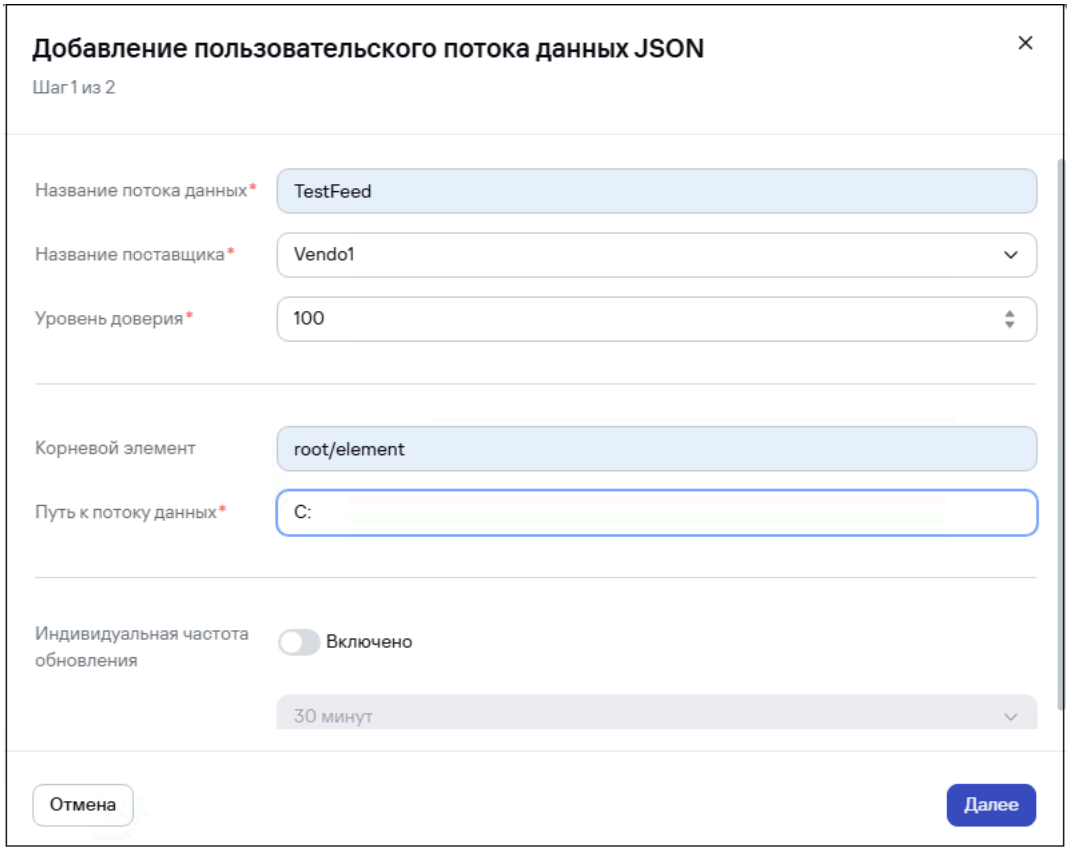
- Для STIX 1.0 или 1.1 следует выбрать «1»
- Для STIX 2.0 следует выбрать «2»
- Для STIX 2.1 следует выбрать «2.1»

- **CSV**
- **XML**
- **MISP**
- **Электронная почта**

  Дополнительная информация о потоках данных об угрозах типа «электронная почта» приведена в разделе Добавление пользовательского или стороннего потока данных об угрозах типа «электронная почта».

- **PDF**

Откроется окно для добавления пользовательского потока данных:



Добавление пользовательского или стороннего потока данных об угрозах

3. Для любого пользовательского или стороннего потока данных об угрозах необходимо указать следующую информацию:

   - **Название потока данных**

     В имени потока данных об угрозах можно использовать латинские буквы, цифры, знаки подчеркивания и дефисы. Имя не должно совпадать с другими уже используемыми именами потоков данных об угрозах.

В качестве имени потока данных об угрозах не следует использовать *FalsePositive* или *InternalTI*, поскольку эти имена зарезервированы для встроенных имен источников данных об угрозах Kaspersky CyberTrace.

Не используйте символ @ в имени потока данных об угрозах.

- **Название поставщика**

  В раскрывающемся списке выберите имя поставщика потока данных об угрозах или добавьте нового.

- **Уровень доверия**

  Уровень доверия к источнику данных об угрозах. Это поле не может быть пустым. Диапазон возможных значений — от 1 до 100.

  По умолчанию заданы значения: `100` для потоков данных об угрозах «Лаборатории Касперского», `50` для потоков данных об угрозах OSINT и `50` для сторонних потоков данных об угрозах. Эти значения можно изменить.

  Уровень доверия указывается в атрибуте `Feeds > Feed > confidence` конфигурационного файла Kaspersky CyberTrace Service.

- **Путь к потоку данных**

  > Для потоков данных об угрозах в формате PDF разрешается указывать только локальный каталог или сетевую папку в качестве пути в Windows.

  Пользовательские потоки данных хранятся в разрешенных каталогах, которые вы можете указать в конфигурационном файле. Укажите путь к пользовательским потокам данных одним из следующих способов:

  - Полный путь к хосту, на котором установлен Kaspersky CyberTrace.

    При добавлении или изменении пользовательского потока данных пользователи с ролью "Администратор" могут задавать собственные разрешенные каталоги для хранения пользовательского потока данных, добавляя их в конфигурационный файл `bin/kl_feed_service.conf`, который находится в разделе `Configuration/ServiceSettings/Security/CustomFeedsSecurity/AllowedDirectories`.

    После добавления разрешенной каталоги Kaspersky CyberTrace нормализует и проверяет путь к ней.

    Каталог по умолчанию для Windows: `%path%/Kaspersky CyberTrace/custom_feeds`.

    Каталог по умолчанию для Linux: `%path%/ktfs/custom_feeds`.

    `%path%` – это абсолютный путь к каталогу, содержащему каталог CyberTrace.

    Для обновления разрешенных каталогов необходимо остановить работу службу Kaspersky CyberTrace, внести изменения в конфигурационный файл, а затем повторно запустить службу Kaspersky CyberTrace. Если вы измените конфигурационный файл во время работы Kaspersky CyberTrace Service, обработка изменений не гарантирована.

  - Сетевой путь

    Указанный сетевой путь доступен для активной учетной записи пользователя, в то время как Kaspersky CyberTrace Service и Feed Utility работают под учетной записью LocalService. Таким образом, если требуется загружать пользовательские сторонние потоки данных об угрозах из сетевого каталога, предоставьте учетной записи пользователя LocalService доступ к этому сетевому каталогу.

    Пути SMB требуется указать не только для общих, но и для разрешенных каталогов.

    Сетевой каталог должен быть подключенным.

Пример сетевого пути: `\\FileCluster01\Security\Feeds`.

> Указать сетевой путь можно только в Windows.

- Адрес HTTP(S)

  Потоки данных об угрозах Kaspersky Threat Data Feeds и инкрементные потоки данных об угрозах, которые не были добавлены на момент выпуска продукта, можно загрузить по адресу https://wlinfo.kaspersky.com. Сведения о инкрементных потоках данных об угрозах приведены в подразделе «Загрузка инкрементных потоков данных об угрозах» раздела Работа с потоками данных об угрозах.

  > Можно использовать адрес IPv4 или IPv6. Адрес IPv6 должен быть заключен в квадратные скобки. Более подробные сведения см. в RFC 2732.

- Адрес FTP

- **Прокси**

  Вы можете включить прокси-сервер для обновления потоков данных об угрозах.

- **Пользовательская частота обновления**

  Вы можете указать отдельную частоту обновления для каждого пользовательского потока данных и OSINT feed.

- **Файл сертификата**

  Путь к сертификату, предоставляющему доступ к потоку данных об угрозах. Необходимо указывать полный путь.

  > Путь к сертификату можно указать, только если поток данных об угрозах будет загружаться через HTTPS-соединение.

  Если потоки данных об угрозах Kaspersky Threat Data Feeds загружаются с ресурса https://wlinfo.kaspersky.com, поле содержит предустановленное значение `Kaspersky Lab certificate`. Это значение изменить невозможно.

- **Тип аутентификации**

  Этот параметр отображается после указания пути к потоку данных.

  Возможные значения типа аутентификации — **Базовый** или **Нет**.

  Базовая схема аутентификации доступна, если путь к потоку данных об угрозах представляет собой адрес HTTP(S) или FTP. Для этого типа аутентификации необходимо ввести следующие настройки:

  - **Имя пользователя**

    Это поле не может быть пустым.

  - **Пароль**

  Тип аутентификации указывается в параметре `Settings > Feeds > Feed` конфигурационного файла Feed Utility.

4. Для потока данных об угрозах STIX также необходимо указать следующую информацию:

- **Сервер TAXII**

  Если этот переключатель включен, то поток данных об угрозах STIX должен загружаться с сервера TAXII™.

  Для потока данных об угрозах STIX 2.0 необходимо указать сервер TAXII 2.0. Для потока данных об угрозах STIX 2.1 необходимо указать сервер TAXII 2.1.

  Если поток данных об угрозах STIX загружается с сервера TAXII, Kaspersky CyberTrace выполняет парсинг этого потока данных об угрозах и подсчитывает количество индикаторов.

- **Название коллекции**

  Имя коллекции, которую необходимо загрузить с сервера TAXII. Обратите внимание, что одновременно можно указать только одно имя коллекции.

  > Kaspersky CyberTrace не поддерживает потоки данных об угрозах TAXII, содержащие информацию о репутации одного объекта. Потоки данных об угрозах IBM, такие как xfe.ipr и xfe.url, не поддерживаются.

5. Для потоков данных об угрозах CSV, XML и JSON укажите следующую информацию:

- Для потоков данных CSV необходимо указать символ-разделитель столбцов. Длина разделителя должна быть равна одному символу, исключениями являются `\n` и `\t`. По умолчанию в качестве разделителя используется точка с запятой (;). Запрещено использовать в качестве разделителей символы решетки (#), кавычки (") и табуляции.

  После этого правило будет применено немедленно, а столбцы будут разделены.

  Для потока данных CSV можно включить или выключить игнорирование заголовка потока данных. По умолчанию заголовок потока данных не игнорируется. Включение игнорирования заголовка потока данных при добавлении потока данных CSV позволяет избежать ложных индикаторов, которые могут возникать из-за заголовка.

  Строки файла CSV-потока данных, начинающиеся с символа решетки (#), считаются комментариями и пропускаются.

  Если включено игнорирование заголовка потока данных, пропускается первая непустая строка, начинающаяся с любого символа, кроме символа решетки (#).

  Строка считается пустой, если она либо полностью пуста (не содержит даже пробелов), либо содержит только пробелы и (или) символы табуляции, либо содержит только пробелы и (или) символы-разделители.

- Для потока данных об угрозах XML можно указать корневой элемент. Это позволяет использовать имена элементов потока данных об угрозах относительно корневого элемента. Элемент, указываемый в качестве корневого, зависит от уровня вложенности в данном потоке данных об угрозах.

  В выражении пути нельзя использовать подстановочные знаки (звездочку «*» или вопросительный знак «?»), а только корневой элемент.

- Для потока данных об угрозах JSON можно указать корневой элемент.

  Значение корневого элемента можно указать с любым уровнем вложенности. Для определения пределов уровня вложенности используется символ « / ».

  Параметр «Root element» может быть пустым. Если он не пустой, значение корневого элемента не должно содержать пустых уровней вложенности (подстрока « / / »), а также не должно начинаться или заканчиваться символом « / ».

  В корневом элементе для потоков данных об угрозах JSON нельзя использовать подстановочные знаки.

В следующем примере демонстрируется корневой элемент для потока данных об угрозах XML, где корневым элементом является `root`:

```
<root>
    <url>http</url>
    <ip>1</ip>
    <url>https</url>
    <ip>2</ip>
</root>
```

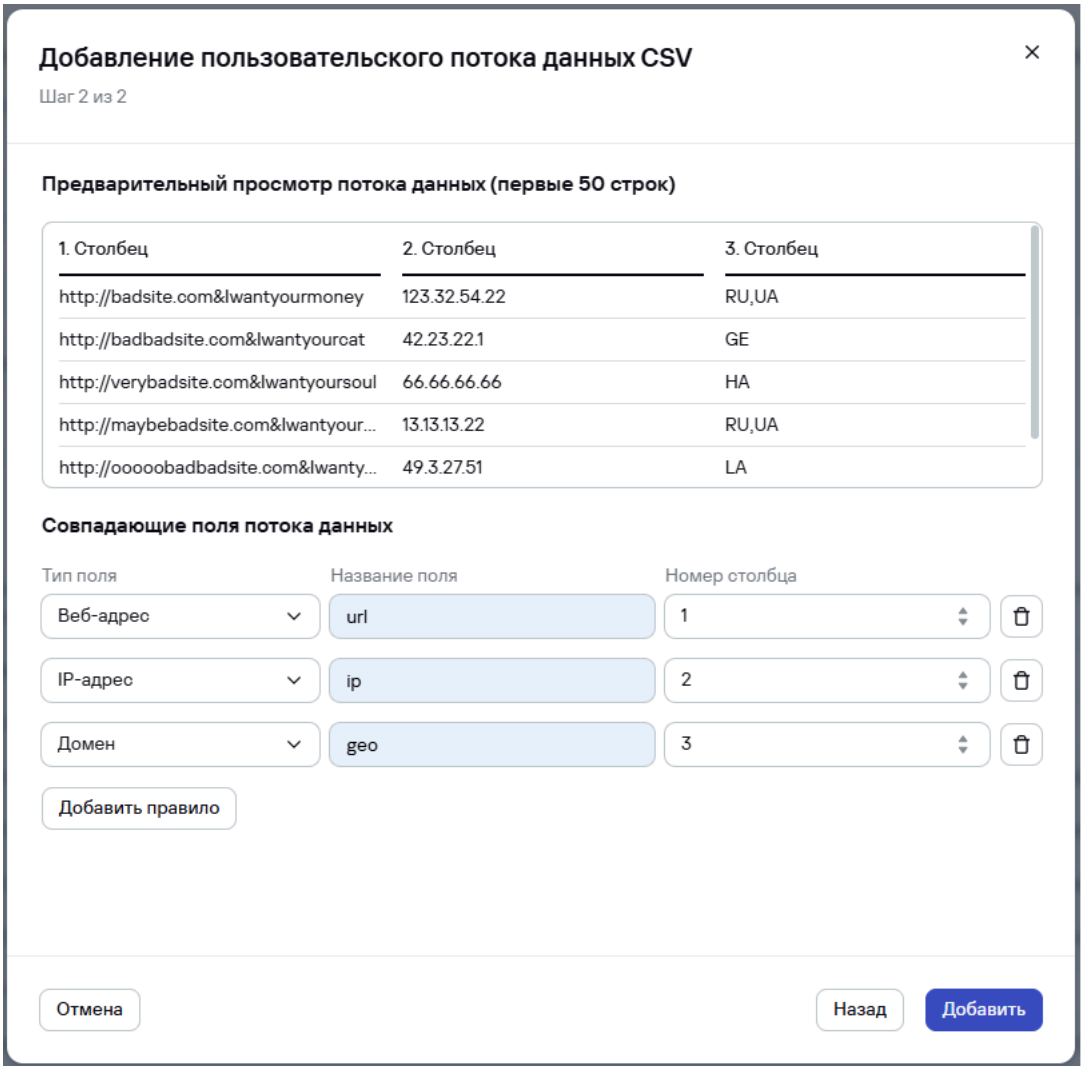
В следующем примере демонстрируется корневой элемент для потока данных об угрозах XML, где корневым элементом является `root/element*`:

```
<root>
    <element1>
        <url>http</url>
        <ip>1</ip>
    </element1>
    <element2>
        <url>https</url>
        <ip>2</ip>
    </element2>
</root>
```

В следующем примере демонстрируется корневой элемент потока данных об угрозах JSON для получения индикаторов IP из поля `ip`, где корневым элементом является `items/ipv4`:

```
{
    "id": 4321,
    "items": [
        {
            "dateDetected": "2022-01-01T01:23:45+00:00",
            "dateLastSeen": "2022-05-28T12:34:56+00:00",
            "ipv4": [
                {
                    "asn": "AS123456, LLC",
                    "city": "Moscow",
                    "countryName": "Russian",
                    "ip": "192.0.0.144"
                },
                {
                    "asn": "AS654321, LLC",
                    "city": "Moscow",
                    "countryCode": "RU",
                    "countryName": "Russian",
                    "ip": "191.0.0.145"
                }
            ],
            "ipv6": []
        },
        ...
    ]
}
```

После указания первоначальных параметров пользовательского или стороннего потока данных об угрозах данный поток полностью загружается, и отображаются его первые 50 строк для того, чтобы можно было выбрать поля, которые должны будут использоваться в процессе сопоставления (см. подраздел «Настройка полей потока данных об угрозах, используемых для сопоставления (потоки данных об угрозах CSV, JSON, XML и PDF)» ниже).



Выбор полей потока данных об угрозах для сопоставления

Это актуально для потоков данных об угрозах в следующих форматах: CSV, JSON или XML. После добавления потока данных об угрозах в формате STIX или потока данных об угрозах Kaspersky, CyberTrace полностью загружает его для использования без необходимости ручной конфигурации полей.

Для потоков данных об угрозах типа PDF или Email можно нажать «Check parsing», чтобы проверить настройки парсинга PDF файлов или E-mail сообщений (включая вложения).

Отобразятся первые 50 строк итогового потока данных об угрозах, в том числе индикаторы тела и вложений обработанных сообщений.

В некоторых случаях, например, когда размер потока данных об угрозах STIX слишком велик и (или) когда сервер TAXII, используемый для загрузки потока данных об угрозах, работает слишком медленно, Kaspersky CyberTrace может затрачивать на загрузку потока данных об угрозах STIX до часа.

После добавления потока данных об угрозах PDF обновите значение `Retention period` (по умолчанию 365 дней).

Настройка полей потока данных об угрозах, используемых для сопоставления (потоки данных об угрозах CSV, JSON, XML и PDF)

При выборе полей для сопоставления из инкрементных потоков данных об угрозах следует игнорировать все поля внутри элемента `metadata`.

Чтобы выбрать поля потока данных об угрозах, которые будут использоваться для сопоставления, укажите следующую информацию для каждого поля:

- **Тип поля**

  В качестве типа поля можно использовать одно из следующих значений:

  - **Веб-адрес**
  - **MD5**
  - **SHA1**
  - **SHA256**
  - **IP-адрес**
  - **Домен**
  - **Контекст**

    Обратите внимание, что хотя бы одно поле должно иметь тип, отличный от **Контекст**. Такие поля используются для сопоставления. Когда такое поле используется в процессе обнаружения киберугроз, генерируется оповещение об обнаружении индикаторов компрометации с категорией `%FEED_NAME%_%FIELD_TYPE%`, где `%FEED_NAME%` — имя потока данных, а `%FIELD_TYPE%` — тип поля.

    Обратите внимание, что для одного потока данных об угрозах можно добавить только одно поле типа URL или DOMAIN.

Укажите все поля **Контекст**, которые требуется добавить в индикатор Kaspersky CyberTrace. Чтобы правильно указать поля обнаружения и контекста для потока данных об угрозах, загруженного с https://wlinfo.kaspersky.com, обратитесь по адресу intelligence@kaspersky.com.

- **Название поля**

  Это имя поля будет использоваться в процессе сопоставления.

  В имени поля можно использовать латинские буквы, цифры, знаки подчеркивания и дефисы. Имя должно содержать хотя бы одну латинскую букву.

- **Регулярное выражение**

  В этом поле укажите регулярное выражение для потока данных об угрозах PDF, которое должно использоваться в качестве правила парсинга.

  Для индикаторов URL и IP (потоки данных об угрозах типа PDF) заданное регулярное выражение настраивается для получения индикаторов, в значении которых есть точка, заключенная в квадратные скобки (например: badurl[.]com).

В Kaspersky CyberTrace, начиная с версии 4.2, регулярные выражения для MD5, SHA1 и SHA256 могут извлекать фрагменты значений из более длинных индикаторов (например, более длинных хешей или URL, если они состоят из символов `a-f` и цифр). Рекомендуется заменить предустановленные регулярные выражения для MD5, SHA1 и SHA256 более конкретными. Например, для MD5 можно использовать `[^\da-fA-F]([\da-fA-F]{32})[^\da-fA-F]` вместо `([\da-fA-F]{32})`.

- Ссылка на данные в потоке данных об угрозах:

  - Для потока данных об угрозах CSV укажите номер столбца.

  - Для потока данных об угрозах JSON укажите имя поля.

    Укажите полный путь к элементу относительно корневого элемента. В выражении пути нельзя использовать ни подстановочные знаки (звездочку «*» или вопросительный знак «?»), ни корневой элемент.

    > В случае потоков данных об угрозах JSON имя поля чувствительно к регистру. Имена полей следует указывать в том же регистре, в котором они используются в потоке данных об угрозах JSON.

    Для указания вложенного поля, используется косая черта (`/`): например, `mainField/subField`.

  - В случае потока данных об угрозах XML указывается элемент.

    Укажите полный путь к элементу относительно корневого элемента. В выражении пути нельзя использовать подстановочные знаки (звездочку «`*`» или вопросительный знак «`?`»), а только корневой элемент. Путь чувствителен к регистру.

    В следующем примере, если в качестве корневого элемента был указан `root/element*`, то полный путь к элементам относительно корневого элемента — это `url` и `ip`, а не `root/element1/url` или `root/element2/ip`:

```
<root>
    <element1>
        <url>http</url>
        <ip>1</ip>
    </element1>
    <element2>
        <url>https</url>
        <ip>2</ip>
    </element2>
</root>
```

> При добавлении пользовательского или стороннего потока данных об угрозах может выполняться обновление потоков данных об угрозах. В этом случае выдается уведомление об этом, и новый поток данных об угрозах не добавляется. Рекомендуется подождать, а затем попытаться добавить потока данных об угрозах еще раз.

Добавление пользовательского или стороннего потока данных об угрозах типа «электронная почта»

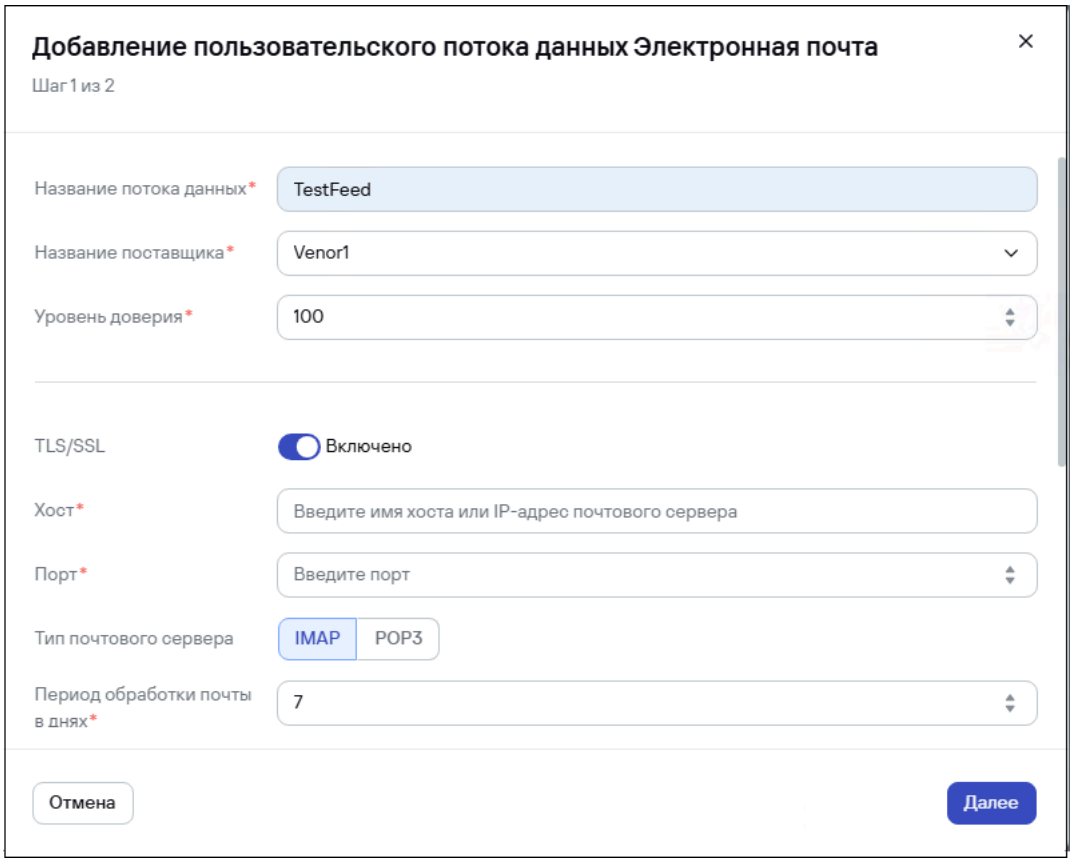
В этом разделе описывается порядок добавления пользовательского или стороннего потока данных об угрозах типа «электронная почта» и изменение его параметров.

Из-за ограничений, налагаемых уровнем лицензирования, эта функция может быть отключена.

Чтобы добавить пользовательский поток данных, выполните следующие действия:

1. На странице **Параметры** → **Потоки данных** нажмите **Добавить пользовательский поток данных**.
2. Выберите тип потока данных **Электронная почта**.

   Откроется окно для добавления пользовательского потока данных типа «электронная почта»:



Добавление потока данных об угрозах типа «электронная почта»

3. Для потока данных об угрозах типа «электронная почта» укажите следующую информацию:

   - **Название потока данных**

     В имени потока данных можно использовать латинские буквы, цифры, знаки подчеркивания и дефисы. Имя не должно совпадать с другими уже используемыми именами потоков данных об угрозах.

     В качестве имени потока данных об угрозах не следует использовать «FalsePositive» или «InternalTI», поскольку эти имена зарезервированы для встроенных имен источников данных об угрозах Kaspersky CyberTrace.

     В имени потока данных об угрозах не следует использовать символ «@», если используется базовая аутентификация, а имя пользователя или пароль содержат «@».

- **Название поставщика**

  В раскрывающемся списке выберите или введите название поставщика потока данных.

- **Уровень доверия**

  Уровень доверия к источнику данных об угрозах. Это поле не может быть пустым. Диапазон возможных значений — от 1 до 100.

  По умолчанию заданы значения: `100` для потоков данных об угрозах «Лаборатории Касперского», `50` для потоков данных об угрозах OSINT и `50` для сторонних потоков данных об угрозах. Эти значения можно изменить.

- **TLS/SSL**

  Включение TLS/SSL позволяет использовать сертификаты TLS/SSL при взаимодействии с почтовым сервером.

  По умолчанию TLS/SSL включен. Отключите переключатель, если почтовый сервер не использует TLS/SSL.

- **Хост**

  Имя хоста или IP-адрес почтового сервера, к которому требуется подключаться. Это поле не может быть пустым.

- **Порт**

  Порт почтового сервера, к которому требуется подключаться. Это поле не может быть пустым.

- **Тип почтового сервера**

  Протокол взаимодействия с почтовым сервером. Выберите POP3 или IMAP. По умолчанию выбран протокол IMAP.

- **Период обработки почты в днях**

  Количество дней, необходимое для обработки сообщений с почтового сервера.

  Необходимо указать целое положительное число. Максимальное значение: 365. По умолчанию задано значение 7.

- **Имя пользователя**

  Учетная запись для подключения к почтовому серверу. Это поле не может быть пустым.

- **Пароль**

  Пароль учетной записи для подключения к почтовому серверу. Это поле не может быть пустым.

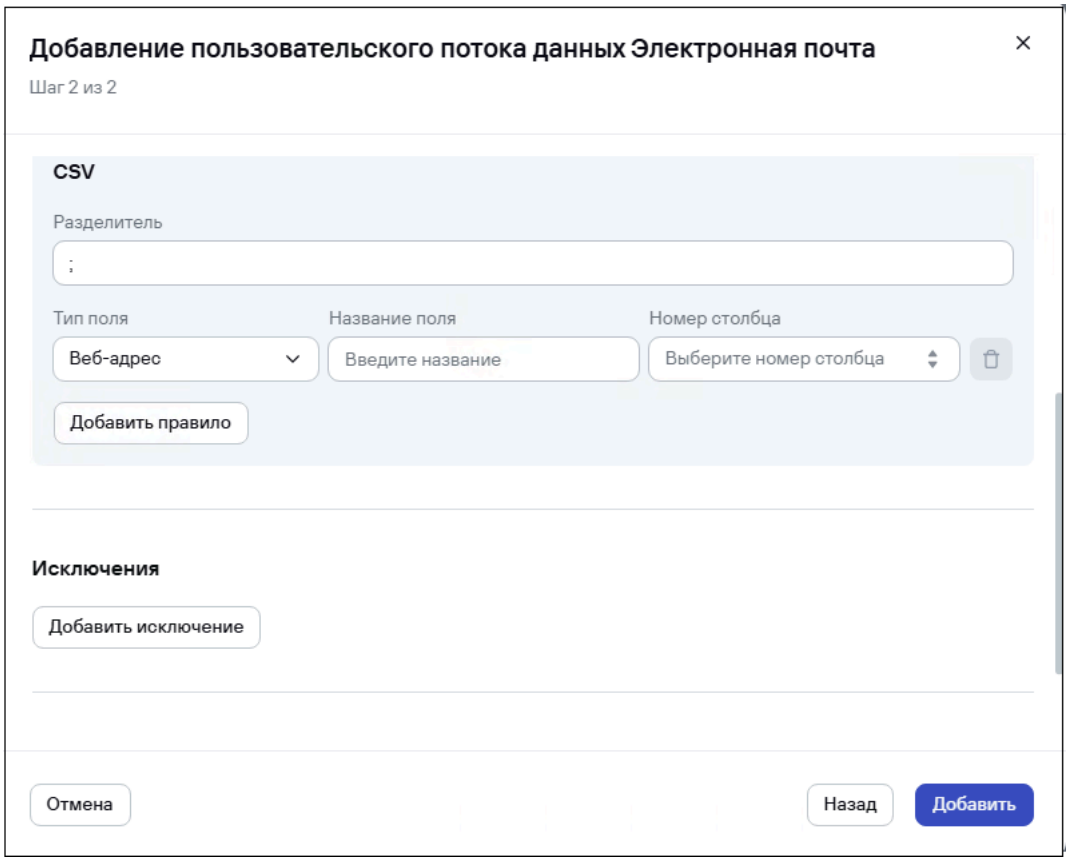
- **Проверить соединение**

  Нажмите на кнопку **Проверить соединение**, чтобы подключиться к почтовому серверу. Результат отображается во всплывающем окне.

После заполнения вышеуказанных полей нажмите кнопку **Далее**, чтобы перейти к следующему окну настройки, затем укажите правила фильтрации для сообщений электронной почты и правила парсинга для тела и вложений сообщений.

После добавления потока данных об угрозах типа «электронная почта» обновите значение `Retention period` (по умолчанию 365 дней).

В следующем окне отображаются поля для настройки правил фильтрации и парсинга:



Правила фильтрации и парсинга

Добавление фильтров сообщений

Фильтры сообщений задают правила выбора сообщений электронной почты для парсинга. Сообщения электронной почты могут выбираться по теме и по отправителю. Во всех правилах используется оператор конъюнкции («AND»).

Чтобы добавить фильтры сообщений, выполните следующие действия:

1. В разделе **Правила фильтрации электронной почты** нажмите на кнопку **Добавить правило**.

   Можно добавить одно или несколько правил. Если не добавлено ни одно правило, парсингу подвергаются все сообщения электронной почты с сервера.

2. Для каждого поля указывается следующая информация:

   - **Поле**

     Правила фильтрации можно применить к одному из следующих полей сообщения электронной почты:

     - **От**

       Отправитель сообщения электронной почты.

     - **Тема**

       Тема сообщения электронной почты.

   - **Условие**

Выберите одно из следующих значений:

- **Содержит** (по умолчанию)

  Значение из сообщения электронной почты должно содержать значение из этого поля.

  Это значение задано по умолчанию.

- **Не содержит**

  Значение из сообщения электронной почты должно не содержать значения из этого поля.

- **Совпадает с**

  Значение из сообщения электронной почты должно быть равно значению из этого поля.

- **Не совпадает с**

  Значение из сообщения электронной почты должно быть не равно значению из этого поля.

- **Значение**

  Критерий, используемый для фильтрации сообщений электронной почты с почтового сервера.

  Это поле не может быть пустым.

Почтовый сервер формирует поле **От** в двух вариантах: **sender@mail.ru** или **sender<sender@mail.ru>**.

Если в **Поле** выбрано **От**, а в **Условие** выбрано **Совпадает с**, значение **Значение** сравнивается со значением **sender@mail.ru** (если в поле **От** задано **sender@mail.ru**), либо сравнение выполняется со значением в круглых скобках (если в поле **От** задано **sender<sender@mail.ru>**).

Настройка правил парсинга вложения сообщения

Эти правила содержат настройки для типов вложений, а также регулярные выражения для парсинга индикаторов и контекста вложений.

Чтобы задать правила парсинга вложений сообщений, выполните следующие действия:

1. Перейдите в раздел **Сообщение**, затем выберите **Вложения**.

   Парсинг вложений сообщения активен по умолчанию. Можно применить один или несколько типов вложений. Вложение одного типа можно применить только один раз.

2. Укажите поля, которые зависят от выбранного типа вложения.

   - **Формат вложения**

     Выберите тип вложения. В качестве типов вложения можно использовать одно или несколько из следующих значений:

     - csv

       Для вложений CSV необходимо указать символ-разделитель столбцов. Длина разделителя должна быть равна одному символу, исключениями являются `\n` и `\t`. По умолчанию в качестве разделителя используется точка с запятой (;).

       Задаются следующие поля: **Тип поля**, **Название поля**, **Номер столбца**.

     - JSON

       Задаются следующие поля: **Тип поля**, **Название поля**, **Корневой элемент**.

- stix1

  Если в настройках потока данных об угрозах типа «электронная почта» одновременно указаны правила парсинга для stix1 и xml, сначала выполняется парсинг файла stix1.

  Если парсинг файла stix1 прошел без ошибок, дальнейшая обработка этого файла в качестве обычного файла XML не выполняется.

- stix2

  Если в настройках потока данных об угрозах типа «электронная почта» одновременно указаны правила парсинга для stix2 и json, сначала выполняется парсинг файла stix2.

  Если парсинг файла stix2 прошел без ошибок, дальнейшая обработка этого файла в качестве обычного файла JSON не выполняется.

- pdf

  В разделе **Вложения** задаются следующие поля: **Тип поля**, **Название поля**, **Регулярное выражение**.

  В поле **Регулярное выражение** можно выбрать предустановленные регулярные выражения или, при необходимости, скорректировать их.

  Для индикаторов URL и IP заданное регулярное выражение настраивается для получения индикаторов, в значении которых есть точка, заключенная в квадратные скобки (например: badurl[.].com).

  В Kaspersky CyberTrace, начиная с версии 4.2, регулярные выражения для MD5, SHA1 и SHA256 могут извлекать фрагменты значений из более длинных индикаторов (например, более длинных хешей или URL, если они состоят из символов `a–f` и цифр). Рекомендуется заменить предустановленные регулярные выражения для MD5, SHA1 и SHA256 более конкретными. Например, для MD5 можно использовать `[^\da-fA-F]([\da-fA-F]{32})[^\da-fA-F]` вместо `([\da-fA-F]{32})`.

- xml

  Для вложения XML необходимо указать корневой элемент. Это позволяет использовать имена элементов потока данных об угрозах относительно корневого элемента. Элемент, указываемый в качестве корневого, зависит от уровня вложенности в данном потоке данных об угрозах. Пример корневого элемента для потока данных об угрозах типа XML приведен в шаге 4 раздела Добавление пользовательского или стороннего потока данных об угрозах.

  В разделе **Вложения** задаются следующие поля: **Тип поля**, **Название поля**, **Элемент**.

- **Тип поля**

  Выберите тип индикатора.

  Это поле недоступно для stix1 и stix2.

- **Название поля**

  Это имя поля будет использоваться в процессе сопоставления.

  В имени поля можно использовать латинские буквы, цифры, знаки подчеркивания и дефисы. Имя должно содержать хотя бы одну латинскую букву.

  Это поле недоступно для stix1 и stix2.

- **Корневой элемент**

  Укажите корневой элемент для типов вложения JSON и XML. Можно указать значение корневого элемента с любым уровнем вложенности. Пределы уровня вложенности задаются с помощью символа « / ».

  Параметр «Root element» может быть пустым. Если он не пустой, значение корневого элемента не должно содержать пустых уровней вложенности (подстрока « // »), а также не должно начинаться или заканчиваться символом « / ».

В корневом элементе для потоков данных об угрозах JSON нельзя использовать подстановочные знаки.

3. Если требуется применять правила исключения в разделе **Исключения**, следует использовать регулярные выражения.

4. Нажмите **Проверить парсинг**, чтобы проверить настройки парсинга вложений.

   Отобразятся первые 50 строк итогового потока данных об угрозах, в том числе индикаторы тела и вложений обработанных сообщений.

5. Нажмите на кнопку **Добавить**.

Настройка правил парсинга тела сообщения

Эти правила содержат регулярные выражения для парсинга индикаторов и контекста тела сообщения.

Чтобы задать правила парсинга тела сообщений, выполните следующие действия:

1. Перейдите в раздел **Сообщение**, затем перейдите на вкладку **Тело**.

2. Задайте значения следующих полей:

   - **Тип поля**

     Выберите тип индикатора.

   - **Название поля**

     Это имя поля будет использоваться в процессе сопоставления.

     В имени поля можно использовать латинские буквы, цифры, знаки подчеркивания и дефисы. Имя должно содержать хотя бы одну латинскую букву.

   - **Регулярное выражение**

     В поле **Регулярное выражение** можно выбрать предустановленные регулярные выражения или, при необходимости, скорректировать их.

     Для индикаторов URL и IP заданное регулярное выражение настраивается для получения индикаторов, в значении которых есть точка, заключенная в квадратные скобки (например: badurl[.].com).

     В Kaspersky CyberTrace, начиная с версии 4.2, регулярные выражения для MD5, SHA1 и SHA256 могут извлекать фрагменты значений из более длинных индикаторов (например, более длинных хешей или URL, если они состоят из символов `a–f` и цифр). Рекомендуется заменить предустановленные регулярные выражения для MD5, SHA1 и SHA256 более конкретными. Например, для MD5 можно использовать `[^\da-fA-F]([\da-fA-F]{32})[^\da-fA-F]` вместо `([\da-fA-F]{32})`.

     Нажмите **Добавить правило**, чтобы применить еще одно регулярное выражение.

   - **Исключения**

     Если требуется применять правила исключения, следует использовать регулярные выражения.

     Добавьте исключения в разделе **Исключения** нажатием на кнопку **Добавить исключение**.

3. Нажмите **Проверить парсинг**, чтобы проверить настройки парсинга тела сообщения.

   Отобразятся первые 50 строк итогового потока данных об угрозах, в том числе индикаторы тела обрабатываемых сообщений и их вложений.

4. Нажмите на кнопку **Добавить**.

Настройка пользовательского или стороннего потока данных об угрозах

В этом разделе описывается порядок настройки пользовательского или стороннего потока данных об угрозах.

Изменение параметров пользовательского или стороннего потока данных

Чтобы изменить параметры пользовательского или стороннего потока данных об угрозах, выполните следующие действия:

1. На странице **Потоки данных** выберите вкладку, содержащую поток данных, который необходимо настроить.

   Изменить настройки источника данных об угрозах *Пользовательские сведения о киберугрозах* невозможно.

2. Нажмите на кнопку ✎ для потока данных, который требуется изменить.

3. В открывшемся окне **Изменение пользовательского потока данных {{format}}** внесите необходимые изменения.

4. Нажмите на кнопку **Сохранить**.

Изменить можно большинство параметров пользовательского или стороннего потока данных об угрозах, однако его тип изменить невозможно. Например, невозможно превратить поток данных об угрозах CSV в JSON.

Добавление новых полей к пользовательскому или стороннему потоку данных

Если в пользовательский или сторонний поток данных было добавлено новое поле или поля, выполните следующие действия, чтобы эти новые поля начали использоваться в Kaspersky CyberTrace:

- Для потока данных CSV, JSON или XML выполните действия в порядке, описанном в подразделе «Изменение настроек пользовательского или стороннего потока данных» выше, чтобы открыть окно **Изменение пользовательского потока данных {{format}}**. Затем добавьте каждое новое поле, для этого нажмите кнопку **Добавить правило**, затем укажите значения, описанные выше в разделе «Шаг 2. Настройка полей потока данных об угрозах, используемых для сопоставления».

  Если не указать новые поля потока данных об угрозах, они будут содержаться в потоке данных об угрозах, но они не будут отображаться в подразделе **Available fields** и не будут использоваться в процессе сопоставления.

- Для потока данных STIX нажмите на имя потока данных и в подразделе **Доступные поля** выберите новое поле или поля, которые должны использоваться в Kaspersky CyberTrace, затем нажмите кнопку **Сохранить**. Подробнее о правилах фильтрации.

Удаление пользовательского или стороннего потока данных об угрозах

Чтобы удалить пользовательский или сторонний поток данных, выполните действия в следующем порядке:

1. На странице **Потоки данных** выберите вкладку, содержащую поток данных, который необходимо удалить.

   Источник данных об угрозах *Пользовательские сведения о киберугрозах* удалить невозможно.

2. Нажмите на кнопку для потока данных, который требуется удалить, затем нажмите кнопку **Удалить**.

Настройка экспорта индикаторов

Индикаторы можно экспортировать в файл формата CSV, который будет содержать подмножество индикаторов (с дополнительными полями контекста или без них), отфильтрованных по определенным правилам. В этом разделе описывается порядок создания задачи экспорта и настройки данных, которые должны быть включены в результирующий файл.

Из-за ограничений, налагаемых уровнем лицензирования, эта функция может быть отключена.

На странице **Параметры** → **Экспорт индикаторов** отображается список существующих задач экспорта. Для работы с этим разделом необходимо перейти в режим **Управление системой**. Этот режим доступен только пользователям с ролью «Администратор».

На странице **Экспорт индикаторов** можно выполнять следующие действия:

- Добавление новой задачи экспорта.
- Управление существующими задачами экспорта.

  С существующими задачами экспорта можно выполнять следующие действия:

  - Изменение существующих задач экспорта.
  - Удаление существующих задач экспорта.
  - Настройка выполнения задач экспорта по расписанию.
  - Запуск задач экспорта.

Добавление новой задачи экспорта

Чтобы добавить задачу экспорта, выполните следующие действия:

1. Нажмите на кнопку **Добавить задачу**.

   Откроется окно **Добавление задачи экспорта индикаторов**.

2. В разделе **Свойства задачи** укажите следующие настройки для каждого поля:

   - **Название задачи**

     Имя задачи экспорта.

   - **Максимальное количество записей**

     Можно указать максимальное количество индикаторов, которые будут включены в отчет.

     Максимальное возможное значение составляет `1000000`.

     По умолчанию задано значение `50000`.

   - **Частота экспорта**

     Частота обновления (в часах) для формирования отчета. По умолчанию задано значение **24 часа**.

   - **Разделитель**

     Разделитель полей в файле отчета. По умолчанию используется точка с запятой (« **;** »).

3. В разделе **Правила фильтрации** укажите правила фильтрации для полей, которые требуется экспортировать.

   Выполните любое из следующих действий:

   - Чтобы добавить новое правило фильтрации, нажмите кнопку **Добавить правило** и задайте следующие параметры:

     - **Название поля**

       Имя поля, к которому применяются правила фильтрации и (или) которое необходимо экспортировать.

     - **Условие**

       Условие фильтрации, которое применяется к полю.

       Можно настроить скользящий временной диапазон от текущей даты до некоторой предыдущей даты. Выберите условие **диапазон от текущей даты до дней назад** и введите значение от 1 до 365. Например, если в качестве значения этого условия для ежедневного экспорта индикаторов задано `5`, то экспортируются индикаторы за последние 5 дней до текущей даты.

     - **Значение**

       Критерии фильтрации для поля. Это значение должно соответствовать требованиям, указанным в разделе "Работа с индикаторами".

     - **Экспорт поля**

       Включите этот переключатель, если поле необходимо включить в файл отчета.

       По умолчанию это поле не входит в файл отчета.

     - **Название выходного поля**

       Имя выходного поля которое должно содержать значения из экспортируемого поля.

     - **Включать имена столбцов**

       Эта настройка позволяет включить в файл отчета заголовки столбцов.

- **Заключать поля в кавычки**

  Эта настройка позволяет заключить экспортируемые поля в кавычки ("), либо экспортировать поля без кавычек. Значения полей могут экспортироваться некорректно, если они не заключены в кавычки (").

Если указано несколько правил фильтрации, они применяются одновременно (используется логический оператор `AND`).

Если индикатор не имеет поля, к которому требуется применить правила фильтрации, этот индикатор должен экспортироваться.

Если индикатор не имеет указанного поля, в то время как в **Условие** выбрано **value is non-empty**, этот индикатор не экспортируется.

Порядок выходных полей в файле отчета CSV совпадает с порядком полей в веб-интерфейсе Kaspersky CyberTrace.

- Чтобы удалить правило фильтрации, нажмите на значок рядом с соответствующей строкой.

4. При необходимости укажите правила сортировки данных в разделе **Условия сортировки**:

   Выполните одно из следующих действий:

   - Чтобы добавить новое условие сортировки, нажмите кнопку **Добавить условие сортировки** и задайте следующие параметры:

     - **Название поля**

       Укажите поле, которое хотите отсортировать.

     - **Порядок сортировки**

       Значения можно отсортировать в порядке возрастания или убывания. Этот порядок также используется в файле экспорта индикаторов.

       При добавлении нового правила сортировки данных по умолчанию используется сортировка **По возрастанию**.

     Если указано несколько условий сортировки, они применяются одновременно (используется логический оператор `AND`).

   - Чтобы удалить правило фильтрации, нажмите на кнопку рядом с требуемой строкой.

5. В разделе **Ограничение доступа к отчету об экспорте индикаторов** укажите следующую информацию:

   - **Требовать авторизацию для скачивания отчета об экспорте индикаторов**

     Включите этот переключатель, если необходимо ограничить доступ к файлу экспорта индикаторов.

     Если этот параметр включен, укажите учетные данные:

     - **Имя пользователя**

       Имя пользователя для доступа к файлу экспорта индикаторов.

       Это имя пользователя предназначено только для доступа к определенному файлу и не тождественно учетной записи пользователя Kaspersky CyberTrace.

     - **Пароль**

       Пароль для доступа к файлу экспорта индикаторов.

6. Нажмите на кнопку **Далее**.

   Откроется окно предварительного просмотра экспорта. В этом окне отображается таблица с примером экспорта индикаторов.

7. Нажмите на кнопку **Добавить**, чтобы применить заданные настройки.

   Если требуется изменить настройки, указанные на предыдущем шаге, нажмите кнопку **Назад**.

   Если требуется сбросить все настройки и закрыть окно, нажмите кнопку **Отмена**.

Новая задача добавляется в список задач экспорта индикаторов.

Управление существующей задачей экспорта

Чтобы изменить существующую задачу экспорта, выполните следующие действия:

1. В списке задач экспорта индикаторов нажмите на кнопку (**Изменить**) рядом с задачей, которую требуется изменить.

2. Измените настройки, как описано в приведенной выше инструкции.

Измененная задача отображается в списке задач экспорта индикаторов.

Чтобы удалить существующую задачу экспорта, выполните следующие действия:

1. В списке задач экспорта индикаторов нажмите на кнопку (**Удалить**) рядом с задачей, которую требуется удалить.

2. В открывшемся окне подтверждения нажмите кнопку **Удалить**.

Удаленная задача более не отображается в списке задач экспорта индикаторов.

Чтобы включить задачу экспорта индикаторов по расписанию, выполните следующие действия:

В списке задач экспорта индикаторов включите переключатель в столбце **Статус** для задачи, которую требуется включить.

Если этот переключатель выключен, доступ к ранее созданным файлам экспорта индикаторов невозможен.

Чтобы запустить задачу экспорта вручную:

В списке задач экспорта индикаторов нажмите на кнопку **Запустить сейчас** рядом с задачей, которую требуется запустить.

После этого файл с экспортированными индикаторами становится доступным для скачивания по следующему адресу:

```
https://%CyberTrace_WebAddress%/ioc_exports/%iocexport_name%
```

где `%iocexport_name%` – имя указанной задачи экспорта.

Получение файла CSV с помощью запроса GET

Можно получить CSV-файл, содержащий информацию об индикаторах, экспортированных из базы данных в соответствии с параметрами, указанными в задаче экспорта индикаторов.

Чтобы получить файл CSV, выполните следующие действия:

Отправьте запрос типа GET на `https://%CyberTrace_WebAddress%/ioc_exports/%iocexport_name%`.

Здесь `%CyberTrace_WebAddress%` — адрес Kaspersky CyberTrace, а `%iocexport_name%` — имя задачи экспорта индикаторов.

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Если для задачи экспорта индикаторов включена авторизация, эта строка должна содержать учетные данные, указанные в настройках задачи экспорта индикаторов.

Тело запроса

Тело этого запроса пустое.

Пример запроса

Ниже приведен пример запроса.

```
GET https://192.168.2.57/ ioc_exports/ExampleExport
Authorization: Basic dXNlcjpwYXNzd29yZA==
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
Content-Type	`text/csv`	Тип содержимого ответа.
Content-Length	Integer	Размер тела ответа в байтах.
Content-Disposition	`attachment;filename={ioc_export}.csv`	Указывает, что содержимое ответа следует рассматривать как вложение.

Тело ответа

Тело ответа содержит строку CSV с экспортированными данными индикаторов.

```
#Column1;Column2
"Value_1_1";"Value_1_2"
"Value_2_1";"Value_2_2"
…
```

В настройках задачи экспорта индикаторов необходимо указать, должна ли первая строка запроса включаться в ответ. Первая строка начинается с символа «#», за которым следуют имена столбцов. Имена столбцов также указываются в настройках задачи экспорта индикаторов.

Пример ответа

Ниже приведен пример ответа.

```
HTTP/1.1 200 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: text/csv
Content-Length: 99
Content-Disposition: attachment;filename=ExampleExport.csv
#ioc_type;ioc_value
"MD5";"FEAF2058298C1E174C2B79AFFC7CF4DF"
"SHA1";"D01D17F6B13C7255A234F558ED85078EA5DD3F3D"
…
```

Ответы с ошибкой

Ошибочные ответы не содержат описания ошибки. Ошибку можно идентифицировать по статусу ответа.

Пример ошибочного ответа

Ниже приведен пример ошибочного ответа.

```
HTTP.1 500 Internal Server Error
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: text/csv
Content-Length: 0
```

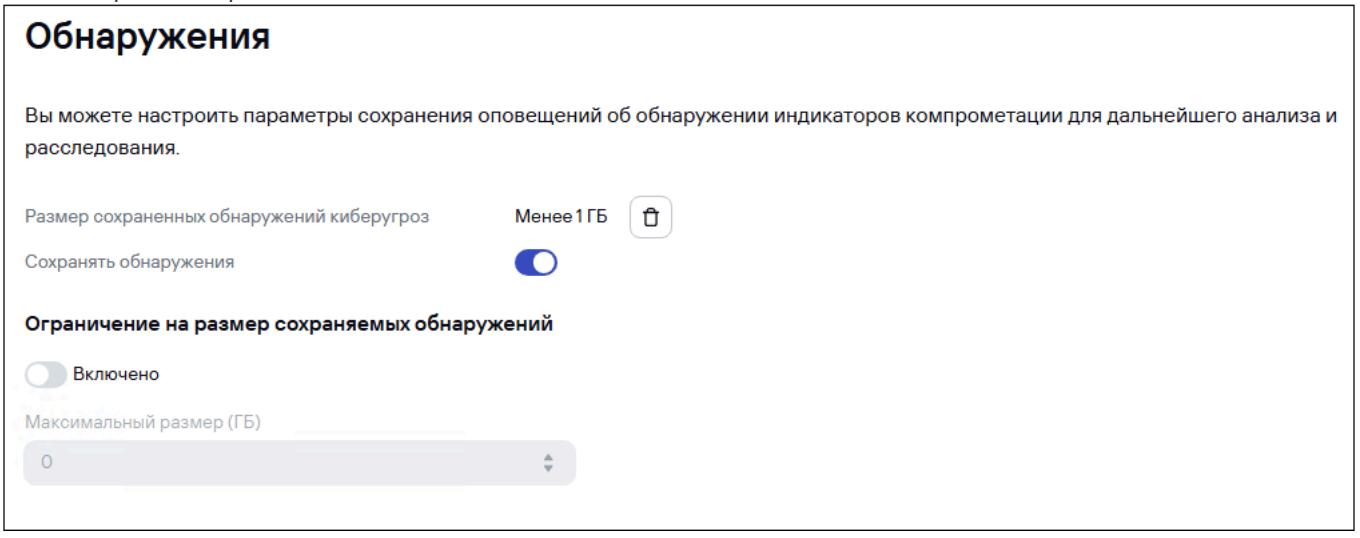
Настройка обнаружения киберугроз

Kaspersky CyberTrace позволяет сохранять исходные оповещения об обнаружении индикаторов компрометации для дальнейшего анализа и расследования. В этом разделе описывается порядок настройки хранилища оповещений об обнаружении индикаторов компрометации.

Для управления параметрами хранилища оповещений об обнаружении индикаторов компрометации используется страница **Параметры** → **Обнаружения**. Для работы с этим разделом необходимо перейти в режим **Управление системой**. Этот режим доступен только пользователям с ролью «Администратор».

Страница **Обнаружения** позволяет выполнять следующие действия:

- Просмотр общего размера сохраненных оповещений об обнаружении индикаторов компрометации.
- Удаление сохраненных оповещений об обнаружении индикаторов компрометации.
- Включение или отключение сохранения оповещений об обнаружении индикаторов компрометации (в т. ч. при ретроспективном сканировании).
- Установка максимального объема (в гигабайтах), отведенного для хранения оповещений об обнаружении индикаторов компрометации.



Страница **Параметры** → **Обнаружения**

Текущий объем (в гигабайтах) сохраненных оповещений об обнаружении индикаторов компрометации отображается в верхней части страницы **Обнаружения**.

Чтобы удалить сохраненные оповещения об обнаружении индикаторов компрометации, выполните следующие действия:

1. Нажмите на значок (**Удалить сохраненные обнаружения киберугроз?**).
2. В открывшемся окне подтверждения нажмите **Удалить**.

Чтобы отключить сохранение оповещений об обнаружении индикаторов компрометации, выполните следующие действия:

1. Выключите переключатель **Сохранять обнаружения**.
2. Нажмите на кнопку **Сохранить** в нижней части страницы.

Отключение сохранения оповещений об обнаружении индикаторов компрометации позволяет уменьшить требования к свободному месту на жестком диске хоста, на котором установлен Kaspersky CyberTrace. Это может быть целесообразно, если все исходные оповещения об обнаружении индикаторов компрометации сохраняются в SIEM-системе и расследование инцидентов безопасности также выполняется в SIEM-системе.

Если отключить сохранение оповещений об обнаружении индикаторов компрометации при применении критериев фильтрации для отправки оповещений в SIEM-системе, то оповещения, содержащие индикаторы, не соответствующие указанным критериям, будут отбрасываться.

Чтобы установить максимальный размер сохраняемых оповещений об обнаружении индикаторов компрометации, выполните следующие действия:

1. Включите переключатель в блоке **Ограничение на размер сохраняемых обнаружений**.
2. Укажите максимальный общий размер сохраняемых оповещений об обнаружении индикаторов компрометации в гигабайтах.
3. Нажмите на кнопку **Сохранить** в нижней части страницы.

При превышении ограничения на размер сохраняемых оповещений об обнаружении индикаторов компрометации Kaspersky CyberTrace генерирует оповещение KL_ALERT_DetectsStorageExceeded.

Поскольку размер сохраненных оповещений об обнаружении индикаторов компрометации проверяется раз в 12 часов, время от времени ограничение может оказываться превышенным. Каждые 12 часов сохраненные обнаружения киберугроз, превышающие лимит, удаляются так, чтобы совокупный размер сохраненных обнаружений киберугроз не превышал лимита.

Работа с тегами

Пользователи Kaspersky CyberTrace могут классифицировать индикаторы угроз с помощью тегов и назначать им приоритеты.

Чтобы приступить к работе с тегами, выполните следующие действия:

Перейдите на страницу **Параметры** → **Теги**. Для работы с этим разделом необходимо перейти в режим **Управление системой**. Этот режим доступен только пользователям с ролью «Администратор».

Теги можно сортировать по имени и по важности в порядке возрастания или убывания.

Добавление тега

Для добавления тега необходимы права администратора.

Чтобы добавить новый тег, выполните следующие действия:

1. Нажмите на кнопку **Добавить тег**.
2. В открывшемся диалоговом окне **Добавление тега** выполните следующие действия:
   a. Задайте имя тега.

      Длина тега должна составлять от 1 до 128 символов. Тег может содержать латинские буквы, цифры, дефисы (-) и знаки подчеркивания (_). Для нового тега нельзя повторно использовать имя уже существующего тега (при сравнении имен тегов регистр игнорируется).

   b. Выберите важность тега.
3. Нажмите на кнопку **Сохранить**.

Созданный тег добавляется в список тегов.

В именах тегов все буквы преобразуются в верхний регистр.

Изменение тега

Чтобы изменить тег, выполните следующие действия:

1. В списке тегов нажмите на кнопку (**Изменить**) рядом с тегом, который требуется изменить.
2. В открывшемся диалоговом окне **Изменение тега** выполните следующие действия:
   a. Если необходимо, укажите новое имя тега.

      В качестве нового имени тега нельзя повторно использовать имя уже существующего тега (при сравнении имен тегов регистр игнорируется).

   b. Выберите важность тега.
3. Нажмите на кнопку **Сохранить**.

Измененный тег выводится в списке тегов.

Поиск тегов

Чтобы выполнить поиск тегов по имени, выполните следующие действия:

В поле поиска введите подстроку для поиска по именам тегов.

Поиск по тегам нечувствителен к регистру.

Удаление тега

Чтобы удалить тег:

1. В списке тегов нажмите на кнопку (**Удалить**) рядом с тегом, который требуется удалить.
2. В открывшемся окне подтверждения нажмите кнопку **Удалить**.

Удаленный тег убирается из списка тегов. Если тег назначен каким-либо индикаторам, Kaspersky CyberTrace снимает тег с этих индикаторов.

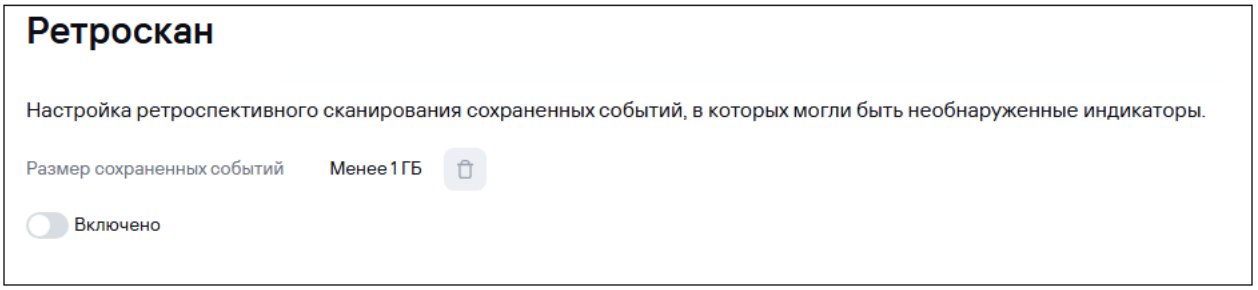
Настройка ретроспективного сканирования

Kaspersky CyberTrace позволяет сохранять события, которые могут содержать необнаруженные индикаторы, выполнять их ретроспективное сканирование по индикаторам из обновленных потоков данных об угрозах и просматривать результаты ретроспективного сканирования. В этом разделе описывается порядок настройки Kaspersky CyberTrace для использования ретроспективного сканирования на странице **Параметры** → **Ретроскан**. Для работы с этим разделом необходимо перейти в режим **Управление системой**. Этот режим доступен только пользователям с ролью «Администратор».

На странице **Ретроскан** можно выполнять следующие действия:

- Включение и выключение ретроспективного сканирования.
- Просмотр текущего объема сохраненных событий.
- Удаление сохраненных событий.

Во время ретроспективного сканирования сохраненные события удалять невозможно. Прежде чем отключить ретроспективное сканирование и удалить сохраненные события, необходимо дождаться завершения текущей задачи ретроспективного сканирования.

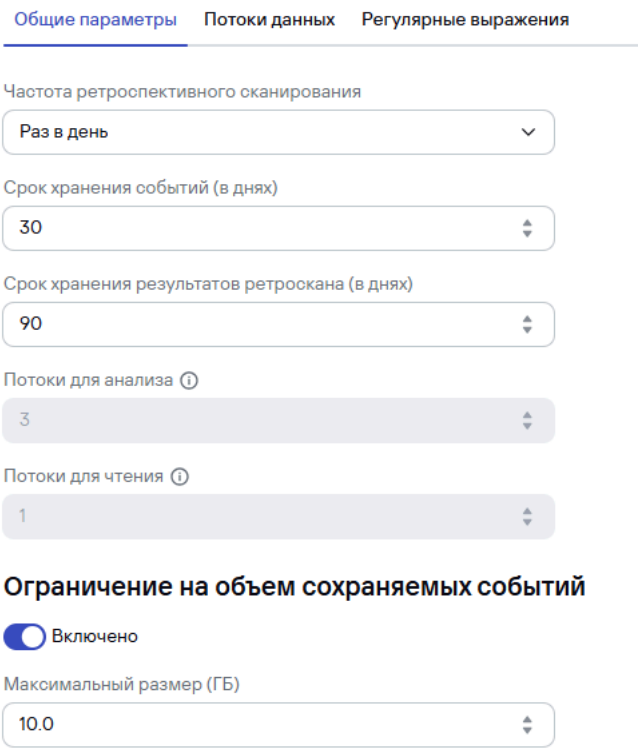


Страница **Ретроскан**

- На вкладке **Общие параметры** задайте следующие настройки:
  - Задайте частоту выполнения задачи ретроспективного сканирования по расписанию или отключите сканирование по расписанию. Если выбран вариант **Раз в месяц**, ретроспективное сканирование запускается каждые 30 дней.
  - Включите или выключите ограничение на размер событий, сохраняемых для ретроспективного сканирования.
  - Установите максимальный объем событий (в гигабайтах), сохраняемых для ретроспективного сканирования.
  - Укажите, как долго (в днях) должны храниться события, используемые для ретроспективного сканирования.
  - Укажите, как долго (в днях) должны храниться результаты ретроспективного сканирования.

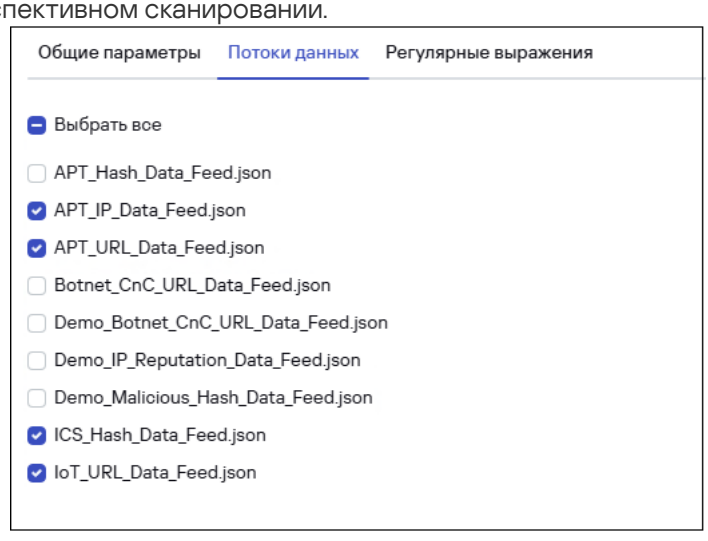
- Просмотрите количество потоков исполнения, выделенных для анализа и считывания сохраненных событий.

  Параметры **Потоки для анализа** и **Потоки для чтения** доступны только для чтения. Изменить количество потоков исполнения, выделенных для анализа и считывания сохраненных событий, можно только в конфигурационном файле Kaspersky CyberTrace Service. Эти параметры задаются в атрибутах `retroscan_task_threads_for_analysis` и `retroscan_task_threads_for_reading` элемента `RetroScan`.



Вкладка **Общие параметры**

- На вкладке **Потоки данных** включите или отключите потоки данных об угрозах, которые требуется использовать при ретроспективном сканировании.



Вкладка **Потоки данных**

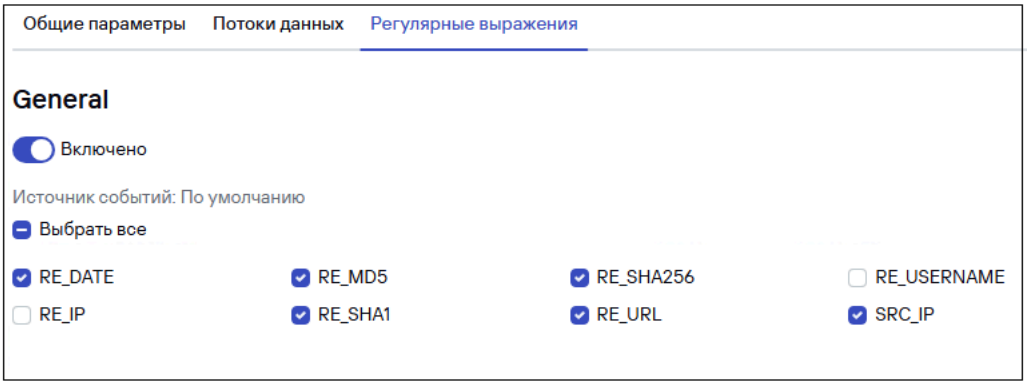
- На вкладке **Регулярные выражения** задайте следующие параметры:

  - Включите или выключите сохранение событий, связанных с конкретным тенантом, для использования в ретроспективном сканировании.

    Если исключить тенант из ретроспективного сканирования, регулярные выражения, содержащиеся в этом тенанте, станут недоступны для выбора.

  - Выберите регулярные выражения, содержащиеся в тенанте, для использования в ретроспективном сканировании.

    Необходимо выбрать хотя бы одно регулярное выражение.



Вкладка **Регулярные выражения**

Рекомендации по настройке ретроспективного сканирования

Ретроспективное сканирование – это ресурсоемкий процесс, который может потребовать много времени, если применять его к огромным объемам данных. Для более эффективного использования ретроспективного сканирования без поиска индикаторов для всех входящих событий рекомендуется выделить события, для которых будет выполняться ретроспективное сканирование, в отдельный источник событий.

Чтобы добавить источник событий для ретроспективного сканирования, выполните следующие действия:

1. Добавьте источник событий.

   При настройке источника событий обратите внимание на следующее:

   - Добавьте регулярное выражение для выделения события (например, для формата события syslog это может быть `^\<d+\>.*$`).

   - Задайте имя правила, характерное для данного источника и типа индикатора (например, `RE_IP_NEW_SIEM`).

     Регулярные выражения для различных источников событий см. в разделе Регулярные выражения для популярных источников событий.

2. Перейдите на страницу **Параметры** → **Ретроскан**, затем выберите вкладку **Регулярные выражения**.

3. Включите только те источники и их регулярные выражения, которые необходимы для ретроспективного сканирования.

4. Сохраните изменения.

Служебные оповещения, связанные с ретроспективным сканированием

Kaspersky CyberTrace генерирует следующие служебные оповещения, чтобы информировать вас о процессе ретроспективной проверки:

- `KL_ALERT_RetroScanCompleted`
- `KL_ALERT_RetroScanError`
- `KL_ALERT_RetroScanStorageExceeded`

Подробную информацию об этих оповещениях см. в разделе Служебные оповещения, отправляемые Kaspersky CyberTrace.

Управление задачами отчетов для передачи отчетов по статистике

Kaspersky CyberTrace позволяет настраивать задачи для рассылки статистических отчетов по электронной почте. В этом разделе объясняется порядок управления задачами для формирования и рассылки отчетов по электронной почте, а также настройка и составление расписания почтовых рассылок.

> Из-за ограничений, налагаемых уровнем лицензирования, эта функция может быть отключена.

Вы можете скачать отчеты в разделе **Информационная панель** или **Отчеты**.

Чтобы загрузить статистические отчеты в разделе **Информационная панель**, у вас должен быть один из следующих уровней лицензирования: Community Edition, Matching Engine, TIP Enterprise.

У пользователей с ролями «Администратор» и «Менеджер тенанта» в рамках лицензии TIP Enterprise есть доступ к разделу **Отчеты**. Для пользователей с ролями «Администратор» и «Менеджер тенанта» в рамках лицензий Community Edition и Matching Engine раздел **Отчеты** отображается в режиме только для чтения. Для пользователей с ролью «Аналитик» раздел **Отчеты** скрыт.

Управление задачами отчетов осуществляется в разделе **Параметры** → **Отчеты**. Для работы с этим разделом необходимо перейти в режим **Управление системой**. Этот режим доступен только пользователям с ролью «Администратор». В этом разделе отображается таблица задач рассылки отчетов. Для каждой задачи приводятся следующие данные:

- **Статус**

  Указывает, включена задача или выключена. В режиме **Управление системой** или в каждом тенанте можно одновременно включить не более трех задач.

- **Название**

  Имя задачи.

- **Создано**

  Имя учетной записи пользователя, добавившего задачу.

- **Электронная почта получателя**

  Адрес электронной почты получателя.

- **Период**

  Периодичность (месяц, неделя, день) и время запуска задачи.

- **Последний запуск задачи**

  Дата и время последнего запуска задачи.

  Предупреждающий знак (⚠) в столбце **Последний запуск задачи** таблицы указывает, что задача завершилась с ошибкой.

- **Следующий запуск задачи**

  Дата и время следующего запуска задачи.

- **Действия**

  Операции, которые можно выполнить с задачей: запуск задачи (**Запустить сейчас**), изменение задачи, удаление задачи, загрузка отчета.

В разделе **Отчеты** можно настроить почтовый клиент, создать задачу отчета и проверить соединение с почтовым сервером.

Настройка почтового клиента

В разделе **Отчеты** можно настроить почтовый клиент для передачи отчетов по статистике.

Чтобы настроить почтовый клиент, выполните следующие действия:

1. В разделе **Параметры** → **Отчеты** нажмите на кнопку **Настройка почтового клиента**.

   Откроется окно **Настройка почтового клиента**.

2. В группе параметров **Параметры соединения** задайте следующие параметры:

   - **Адрес сервера SMTP**

     Укажите адрес сервера SMTP. Можно ввести от 1 до 255 символов.

   - **Порт SMTP-сервера**

     Укажите порт сервера SMTP. Можно ввести значения от 0 до 65535.

   - **Безопасное подключение**

     В раскрывающемся списке выберите вариант **Нет**, **SSL/TLS** или **STARTTLS**.

     Перед установкой шифрованного соединения STARTTLS или SSL/TLS с почтовым сервером, используемым для отправки отчетов, убедитесь, что для этого сервера имеется TLS-сертификат, который добавлен в хранилище доверенных сертификатов на компьютере.

     Этот сертификат можно получить путем обращения к почтовому серверу или в Службу технической поддержки вашей организации.

     Сертификат хранится в директории `/etc/ssl/certs`, которая содержит символьные ссылки на полученный сертификат. Имя ссылки содержит хеш сертификата.

     Чтобы добавить сертификат в хранилище доверенных сертификатов, выполните следующие команды:

     - В ОС Windows:

       ```
       Import-Certificate –FilePath "path/to/mail_server_certificate.crt" -
       CertStoreLocation Cert:\LocalMachine\Root
       ```

- На Linux deb формат имени сертификата задается утилитой `update-ca-certificates`.
- На Linux rpm формат имени сертификата задается пользователем вручную с помощью команды `openssl x509 –in YOUR_CERT_FILE –hash –noout`.

3. В группе параметров **Учетная запись** задайте следующие параметры:

   - **Имя пользователя**

     В поле **Логин** укажите имя учетной записи клиента. Можно ввести от 0 до 64 символов.

   - **Адрес эл. почты**

     В поле **Адрес эл. почты** укажите адрес электронной почты пользователя клиента. Можно ввести от 1 до 254 символов.

   - **Пароль**

     В поле **Пароль** укажите пароль пользователя. Можно ввести от 1 до 128 символов.

   - **Текстовое сообщение**

     При необходимости в поле **Текстовое сообщение** можно ввести сообщение, которое получит пользователь вместе с отчетом. Можно ввести от 0 до 10 000 символов.

4. Нажмите на кнопку **Сохранить**.

Настройки почтового клиента будут применены.

Если требуется закрыть страницу **Настройка почтового клиента** без сохранения данных, нажмите на кнопку **Отмена**.

Создание задачи рассылки отчета

Задачу рассылки отчета можно создать для отправки статистических отчетов по электронной почте и для индивидуальной настройки параметров отчета.

Чтобы создать задачу рассылки отчета и настроить отчет:

1. На странице **Параметры** → **Отчеты** нажмите на кнопку **Добавить задачу**.

   Откроется окно **Добавление задачи отчета**.

2. В группе параметров **Свойства задачи** задайте следующие параметры доставки отчета:

   - В поле **Название задачи** введите имя задачи.
   - В поле **Адрес получателя** введите адрес электронной почты получателя.

     Не более 2048 символов. Поддерживаются только адреса электронной почты с доменными именами, записываемыми латиницей.

   - В поле **Тема сообщения** введите тему письма.
   - В поле **Текстовое сообщение** введите сообщение, если требуется.

3. В группе параметров **Повторять** настройте периодичность рассылки электронной почты, время начала отправки и часовой пояс.

   Время выполнения задачи определяется в соответствии с указанным часовым поясом и отображается в отчетах.

4. Нажмите на кнопку **Далее**.

5. Настройте следующие параметры отчета:

   - В группе параметров **Свойства отчета** задайте следующие параметры:

     - В поле **Источник данных** в раскрывающемся списке выберите в качестве источника данных **TCP**, **Поиск через API** или **Все**.

     - В раскрывающемся списке **Период с** выберите период, статистика за который должна быть отражена в отчете.

     - В раскрывающемся списке **Тенанты** выберите тенанты, чьи данные требуется включить в отчет. Тенанты можно выбирать только в режиме **Управление системой**. В режиме **Управление данными** в отчет включаются только данные того тенанта, в котором выполняется задача.

     - В поле **Язык** выберите язык отчета. По умолчанию используется язык, настроенный в вашей учетной записи.

     - Если требуется включить в отчет ложные срабатывания, установите соответствующий флажок.

   - В группе параметров **Свойства страницы** установите флажки для элементов, которые требуется включить в отчет: титульная страница, логотип "Лаборатории Касперского", имя пользователя и ф. и. о. пользователя.

   - В группе параметров **Виджеты** выберите виджеты, которые требуется включить в отчет.

     - Для виджета **Обзор статистики** можно установить следующие флажки:

       - **Входящие события**

       - **Количество обнаруженных киберугроз**

       - **Количество обнаруженных индикаторов**

     - Для виджета **Топ обнаруженных индикаторов** можно установить следующие флажки:

       - **По умолчанию**

       - **Ретроскан**

       - **Топ-10 хешей**: MD5, SHA1, SHA256

6. Нажмите на кнопку **Сохранить**.

Задача отчета будет создана и добавлена в таблицу задач в разделе **Отчеты**. По умолчанию созданная задача добавляется в таблицу в выключенном состоянии.

Для включения созданной задачи выполните следующие действия:

1. На странице **Параметры** → **Отчеты** нажмите на кнопку **Проверка соединения**.
2. Если соединение успешно установлено, включите переключатель в столбце **Статус** таблицы задач.

   Задача будет включена.

Запуск, редактирование и удаление задачи отчета

Задачу рассылки отчетов можно запустить сразу же, вне настроенного расписания доставки, также задачу можно изменить или удалить.

Запуск задачи отчета

Чтобы запустить задачу рассылки отчетов, выполните следующие действия:

1. Перейдите в раздел **Параметры** → **Отчеты** и проверьте соединение с почтовым сервером, нажав на кнопку **Проверка соединения**.
2. В столбце **Статус** таблицы задач включите переключатель для задачи, которую требуется запустить.
3. В столбце **Действия** нажмите на кнопку **Запустить сейчас**.

   Задача будет выполнена, а отчеты будут доставлены. Во время выполнения задачи эту задачу невозможно отключить, изменить или удалить; также невозможно скачать отчет.

Изменение задачи отчета

Чтобы изменить задачу отчета, выполните следующие действия:

1. Перейдите в раздел **Параметры** → **Отчеты**.
2. В столбце **Действия** таблицы задач нажмите на значок **Изменить** (✎).
3. Измените задачу отчета.

   Подробную информацию о параметрах задач отчетов см. в разделе Создание задачи отчета.
4. Нажмите на кнопку **Сохранить**.

   Задача изменена. Теперь задачу рассылки отчетов можно включить.

Удаление задачи рассылки отчетов

Чтобы удалить задачу рассылки отчетов, выполните следующие действия:

1. Перейдите в раздел **Параметры** → **Отчеты**.
2. В столбце **Действия** таблицы задач нажмите на значок **Удалить** ().
3. В открывшемся окне подтвердите удаление задачи.

Задача будет удалена.

Скачивание отчета

В разделе **Параметры** → **Отчеты** вы можете загрузить отчет по задаче.

Чтобы скачать отчет, выполните следующие действия:

1. Убедитесь, что задача включена, в таблице задач.

   Если задача отключена, используйте соответствующий переключатель в столбце **Статус**, чтобы включить ее.
2. В столбце **Действия** нажмите на значок **Загрузить** ().

Отчет скачивается.

Также вы можете загрузить отчет в разделе **Информационная панель**.

Параметры Безопасность

Kaspersky CyberTrace может сохранять информацию о действиях пользователей в веб-интерфейсе. Информация сохраняется в виде событий в журнале аудита действий пользователей, если в конфигурационном файле включен аудит действий пользователей. Журнал аудита действий пользователей хранится локально на компьютере, на котором установлен Kaspersky CyberTrace. Путь к директории с файлами журнала аудита действий пользователей задается в конфигурационном файле. В случае необходимости в конфигурационном файле можно указать другой каталог.

Аудит действий пользователей доступен только для коммерческих уровней лицензирования и включен по умолчанию.

Для настройки аудита действий пользователей используется страница **Параметры** → **Безопасность**.

Включение и выключение аудита действий пользователей

Вы можете включить или выключить аудит действий пользователей в конфигурационном файле Kaspersky CyberTrace Service. По умолчанию аудит действий пользователей включен.

Если вы отключите аудит действий пользователей, параметры на странице **Параметры** → **Безопасность** будут недоступны.

Чтобы включить или выключить аудит действий пользователей:

1. Откройте файл kl_feed_service.conf для редактирования.

   Местоположение файла kl_feed_service.conf зависит от вашей операционной системы.

2. В разделе `Configuration` → `ServiceSettings` конфигурационного файла найдите элемент `Audit`.

3. Установите для атрибута `enabled` элемента `Audit` одно из следующих значений:

   - `true` – включить аудит действий пользователей.
   - `false` – отключить аудит действий пользователей.

4. Сохраните и закройте файл kl_feed_service.conf.

5. Перезагрузите Kaspersky CyberTrace Service, чтобы изменения вступили в силу.

Настройка аудита действий пользователей

Для настройки аудита действий пользователей используется страница **Параметры** → **Безопасность**. Эти параметры также доступны в конфигурационном файле Kaspersky CyberTrace Service.

Для работы со страницей **Безопасность** необходимо перейти в режим **Управление системой**.

> Эти параметры доступны только для коммерческих уровней лицензирования.

Настройка срока хранения событий

По умолчанию события действий пользователей хранятся в журнале аудита действий пользователей в течение 90 дней, после чего удаляются. Вы можете изменить срок хранения событий действий пользователей или указать неограниченный срок хранения.

Чтобы настроить срок хранения событий действий пользователей:

1. В меню слева перейдите на страницу **Параметры** → **Безопасность**.

2. Выберите вкладку **Параметры аудита**.

3. Если вы хотите хранить все события действий пользователей, не удаляя их, в разделе **Срок хранения событий** включите переключатель **Неограниченный срок хранения**.

4. Если вы хотите хранить события действий пользователей только за определенный период и удалять старые события, в разделе **Срок хранения событий** выполните следующие действия:

   a. Отключите переключатель **Неограниченный срок хранения**.

   b. В поле **Срок хранения (в днях)** укажите, сколько дней события действий пользователей должны храниться в журнале аудита действий пользователей.

      Нельзя указывать период хранения менее 30 дней.

5. Нажмите на кнопку **Сохранить**.

Отправка событий действий пользователей по TCP

При необходимости вы можете включить или отключить отправку событий в другие приложения (например, в SIEM-систему) для дальнейшего анализа. Если этот параметр включен, события будут отправляться по протоколу TCP.

Чтобы включить или отключить отправку событий действий пользователей по TCP:

1. В меню слева перейдите на страницу **Параметры** → **Безопасность**.
2. Выберите вкладку **Параметры аудита**.
3. Если вы не хотите отправлять события действий пользователей в другие приложения, отключите переключатель в разделе **Отправка событий по протоколу TCP**.
4. Если вы хотите отправлять события действий пользователей в другие приложения, в разделе **Отправка событий по протоколу TCP** выполните следующие действия:
   a. Включите переключатель.
   b. В полях **IP-адрес или имя хоста** и **Порт** укажите IP-адрес или имя хоста и порт, на который Kaspersky CyberTrace будет отправлять события действий пользователей.
   c. В поле **Безопасное подключение** выберите тип соединения для отправки событий действий пользователей: **TLS с проверкой сертификата**, **TLS без проверки сертификата** или **Нет**.
5. Нажмите на кнопку **Сохранить**.

Скачивание журнала аудита действий пользователей

Чтобы скачать журнал аудита действий пользователей:

1. В меню слева перейдите на страницу **Параметры** → **Безопасность**.
2. Выберите вкладку **Журнал аудита**.
3. Используйте средство выбора даты в календаре, чтобы выбрать начало и конец периода, для которого вы хотите скачать события действий пользователей.

   Период должен быть меньше или равен сроку хранения для событий действий пользователей.
4. Нажмите на кнопку **Скачать**.

> Если вы выберете период более 90 дней, подготовка файлов журнала аудита действий пользователей может занять некоторое время.

Журнал аудита действий пользователей будет скачан в виде ZIP-архива, содержащего один или несколько файлов CEF. По умолчанию формат имени архива – audit_<дата начала>_<дата окончания>.zip.

О журнале аудита действий пользователей

События действий пользователей сохраняются в журнале аудита локально в виде файлов в формате CEF на компьютере, на котором установлен Kaspersky CyberTrace.

Каждый файл содержит события действий пользователей, записанные за один день. Формат имени файла – audit_<дата>.cef. Если вы укажете срок хранения событий действий пользователей, Kaspersky CyberTrace автоматически удалит старые файлы журналов действий пользователей.

Только Kaspersky CyberTrace имеет доступ, требуемый для чтения, изменения и удаления каталога журнала аудита действий пользователей и файлов, находящихся в нем. Другие пользователи не могут получить доступ к этому каталогу и его содержимому. Если вы хотите просмотреть журнал аудита действий пользователей, вы можете скачать его в веб-интерфейсе Kaspersky CyberTrace.

Формат событий действий пользователей

Каждое событие действий пользователей сохраняется в формате CEF и состоит из *заголовка* и *расширения*.

Заголовок события

В заголовке каждого события действий пользователей имеются следующие поля, разделенные вертикальными чертами (|):

- Формат версии CEF – `CEF:<версия>`.
- Название поставщика. Значение этого поля всегда `Kaspersky`.
- Название приложения. Значение этого поля всегда `CyberTrace`.
- Версия решения. Значение этого поля – текущая версия Kaspersky CyberTrace.
- Класс события.
- Тип события.
- Уровень критичности.

В таблице ниже перечислены возможные классы и типы событий и их уровни критичности.

Классы, типы и уровни критичности событий

Класс события	Описание	Тип события	Уровень критичности
`User`	События, связанные с действиями с учетными записями пользователей.	`User Created`	`Medium`
		`User Deleted`	`Medium`
		`User Updated`	`Medium`
		`Password Updated`	`Medium`
		`User Login`	`Low`
		`User Logout`	`Low`
`Service`	События, связанные с действиями с Kaspersky CyberTrace Service.	`Service Restarted`	`Medium`
		`Service Config Exported`	`Low`
		`Service Statistics Reset`	`Medium`

Класс события	Описание	Тип события	Уровень критичности
ServiceSettings	События, связанные с настройкой Kaspersky CyberTrace Service.	Session Settings Updated	Low
		LDAP Settings Updated	Medium
		EPS Settings Updated	Medium
		Service Alerts Settings Updated	Medium
		Service Alerts Format Updated	Low
		Web Interface Settings Updated	Medium
		Proxy Settings Updated	Medium
		Audit Settings Updated	Medium
		KSN Statement Status Updated	Medium
		Logging Settings Updated	Medium
		Detection Storage Settings Updated	Medium
		Detection Storage Cleared	Medium
License	События, связанные с действиями с лицензиями.	License Key Added	Medium
		Active License Key Deleted	High
ServiceFeeds	События, связанные с действиями с потоками данных.	Feed Update Frequency Updated	Medium
		Custom Feed Added	Medium
		Service Feed Certificate Imported	Medium
		Service Feed Enabled	Medium
		Service Feed Disabled	Medium
		Proxy for Kaspersky Threat Data Feeds Updated	Medium
		Service Feed Updated	Medium
		Service Feed Settings Updated	Medium
		Service Feed Deleted	Medium
Tenant	События, связанные с действиями с тенантами.	Tenant Created	Medium
		Tenant Deleted	Medium
		Tenant Basic Settings Updated	Medium
		Tenant EPS Settings Updated	Medium
		Settings for Tenant Incoming Events Updated	Medium
		Settings for Tenant Detection Alerts Updated	Medium
		Settings for Tenant Service Events Updated	Medium
		Settings for Tenant API Lookup Detections Updated	Medium
		Tenant Statistics Reset	Medium

Класс события	Описание	Тип события	Уровень критичности
TenantSettings	События, связанные с настройкой тенанта.	Tenant Event Source Created	Medium
		Normalization Rules of Tenant Event Source Updated	Medium
		Regular Expressions of Tenant Event Source Updated	Medium
		Tenant Event Source Deleted	Medium
		Format of Tenant Service Alerts Updated	Medium
		Format of Tenant Detection Alerts Updated	Medium
		Filtering of Tenant Detection Alerts Updated	Medium
		Context of Tenant Detection Alerts Updated	Medium
TenantFeeds	События, связанные с действиями с потоками данных в тенанте.	Tenant Feed Enabled	Medium
		Tenant Feed Disabled	Medium
		FalsePositive List Updated	Medium
		InternalTI List Updated	Medium
TenantIndicators	События, связанные с действиями с индикаторами в тенанте.	Indicator Deleted	Medium
		Indicator Enriched	Medium
		Indicator Publications Queried	Medium
		Indicator Tags Updated	Medium
RetroScan	События, связанные с ретросканом.	RetroScan Started	Medium
		RetroScan Events Cleared	Medium
		RetroScan Status Updated	Medium
		RetroScan Settings Updated	Medium
		RetroScan Feeds Updated	Medium
		RetroScan Regular Expressions Updated	Medium
ExternalSources	События, связанные с действиями с внешними источниками.	External Source Created	Low
		External Source Updated	Medium
		External Source Deleted	Medium
IndicatorsExport	События, связанные с экспортом индикаторов.	Indicators Export Task Created	Low
		Indicators Export Task Deleted	Medium
		Indicators Export Task Updated	Medium
		Status of Indicators Export Task Changed	Medium
		Indicators Export Task Started	Medium

Класс события	Описание	Тип события	Уровень критичности
Reporting	События, связанные с действиями с отчетами.	Report Task Created	Low
		Report Task Deleted	Medium
		Report Task Updated	Medium
		Report Task Status Changed	Medium
		Report Task Started	Medium
		Report Generation Started	Medium
		Mail Client Settings Updated	Medium

Расширение события

Все поля расширений событий деятельности пользователей представлены в формате строк < ключ >= < значение >, разделенных пробелом. Если расширение события деятельности пользователей содержит обратную косую черту (\ ), подчеркивание (_) или вертикальную черту (|), они экранируются обратной косой чертой (\ ).

Расширения событий деятельности пользователей могут содержать общие ключи и значения, доступные вне зависимости от типа события, а также ключи и значения, зависящие от типа события.

Пример события

Ниже приведен пример события активности пользователей.

```
CEF:0|Kaspersky|CyberTrace|5.4|User|User Login|Low|rt=2026-09-16T14:44:48.803Z dhost=<имя хоста>
cs1Label=tenantName cs1=System src=<IP-адрес> outcome=succeeded externalId=<идентификатор действия> duser=<имя
пользователя>
```

Общие ключи всех событий действий пользователей

В таблице ниже описаны ключи, доступные в расширениях событий аудита пользователей для всех типов событий.

Общие ключи для всех типов событий

Ключ	Значение
rt	Дата и время регистрации события в Kaspersky CyberTrace (UTC) в формате ISO 8601.
dhost	Имя хоста, на котором работает Kaspersky CyberTrace.
cs1Label	Всегда tenantName.
cs1	Имя тенанта, на котором произошло действие (для режима Управление данными), или System (для режима Управление системой).
suser	Имя пользователя, выполнившего действие
src	IP-адрес, с которого был отправлен запрос на выполнение действия Если используется прокси-сервер, это IP-адрес прокси-сервера.
outcome	Результат действия. Возможные значения: • started – событие зарегистрировано при запуске действия. • succeeded – событие зарегистрировано после успешного завершения действия. • requested – событие зарегистрировано после успешной постановки задачи в очередь в результате действия. • failed – событие зарегистрировано завершения действия с ошибкой.

Ключ	Значение
msg	Описание ошибки, если действие завершилось с ошибкой. Этот ключ присутствует только в том случае, если для ключа outcome задано значение failed.
externalId	Уникальный идентификатор действия в формате GUID. Если два события были зарегистрированы для одного и того же действия (одно событие при запуске действия, а другое – при завершении), они имеют одинаковое значение – externalId.

Класс событий User

Помимо общих ключей и значений, события действий пользователей, принадлежащие классу User, содержат разные ключи и значения, зависящие от типа события.

Тип события User Created

События действий пользователей с типом User Created имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
duser	Имя пользователя созданной учетной записи.
cs2Label	Всегда role.
cs2	Роль, назначенная созданной учетной записи. Возможные значения: • admin • tenantManager • analyst
cs3Label	Всегда assignedTenants.
cs3	Список тенантов, доступных для созданной учетной записи, имена которых разделены запятыми. Значение all, если у пользователя есть доступ ко всем тенантам.

Тип события User Deleted

События действий пользователей с типом User Deleted имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
duser	Имя пользователя удаленной учетной записи.
cs2Label	Всегда role.
cs2	Роль удаленной учетной записи. Возможные значения: • admin • tenantManager • analyst

Тип события `User Updated`

События действий пользователей с типом `User Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
`duser`	Имя пользователя обновленной учетной записи. Если имя пользователя было изменено, значением будет новое имя пользователя.
`cs2Label`	Всегда `oldLogin`.
`cs2`	Имя учетной записи перед обновлением.
`cs3Label`	Всегда `newLogin`.
`cs3`	Имя учетной записи после обновления.
`cs4Label`	Всегда `oldRole`.
`cs4`	Роль учетной записи пользователя перед обновлением. Возможные значения: • `admin` • `tenantManager` • `analyst`
`cs5Label`	Всегда `newRole`.
`cs5`	Роль учетной записи пользователя после обновления. Возможные значения: • `admin` • `tenantManager` • `analyst`
`cs6Label`	Всегда `oldTenants`.
`cs6`	Список тенантов, доступных для учетной записи до обновления, имена которых разделены запятыми. Если у пользователя был доступ ко всем тенантам, значение `all`.
`cs7Label`	Всегда `newTenants`.
`cs7`	Список тенантов, доступных для учетной записи после обновления, имена которых разделены запятыми. Если у пользователя есть доступ ко всем тенантам, значение `all`.

Тип события `Password Updated`

События действий пользователей с типом `Password Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`duser`	Имя пользователя учетной записи, для которой был изменен пароль.

Тип события `User Login`

События действий пользователей с типом `User Login` имеют уровень критичности `Low`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Общий ключ `suser` и его значение отсутствуют в событиях с типом события `User Login`.

Ключи и значения

Ключ	Значение
`duser`	Имя пользователя, выполнившего вход в Kaspersky CyberTrace.

Тип события `User Logout`

События действий пользователей с типом `User Logout` имеют уровень критичности `Low`. Расширения событий этого типа включают только общие ключи и значения.

Класс событий Service

События действий пользователей, принадлежащие классу `Service`, включают в себя события следующих типов и уровней критичности:

- События типа `Service Restarted` с уровнем критичности `Medium`
- События типа `Service Config Exported` с уровнем критичности `Low`
- События типа `Service Statistics Reset` с уровнем критичности `Medium`

События действий пользователей, принадлежащие классу `Service`, включают в расширение только общие ключи и значения, вне зависимости от типа события.

Класс событий ServiceSettings

Помимо общих ключей и значений, события действий пользователей, принадлежащие классу `ServiceSettings`, содержат разные ключи и значения, зависящие от типа события.

События типа `Session Settings Updated`

События действий пользователей типа `Session Settings Updated` имеют уровень критичности `Low`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `oldSessionExtension`.
`cs2`	Время ожидания для сеанса пользователя перед обновлением в случае, если пользователь не активен. Возможные значения: • `asLongAsPossible` • `fewMinutes`
`cs3Label`	Всегда `newSessionExtension`.

Ключ	Значение
cs3	Время ожидания для сеанса пользователя после обновления в случае, если пользователь не активен. Возможные значения: • asLongAsPossible • fewMinutes
cs4Label	Всегда oldIdleTimeoutMinutes. Ключ присутствует, только если для cs2 и cs3 указано значение fewMinutes.
cs4	Время ожидания для сеанса пользователя (в минутах) до обновления в случае, если пользователь не активен. Ключ присутствует, только если для cs2 и cs3 указано значение fewMinutes.
cs5Label	Всегда newIdleTimeoutMinutes. Ключ присутствует, только если для cs2 и cs3 указано значение fewMinutes или только для cs3 указано значение multipleMinutes.
cs5	Время ожидания для сеанса пользователя (в минутах) после обновления в случае, если пользователь не активен. Ключ присутствует, только если для cs2 и cs3 указано значение fewMinutes или только для cs3 указано значение multipleMinutes.

События типа LDAP Settings Updated

События действий пользователей типа LDAP Settings Updated имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
cs2Label	Всегда oldStatus.
cs2	Статус LDAP перед обновлением. Возможные значения: • enabled • disabled
cs3Label	Всегда newStatus.
cs3	Статус LDAP после обновления. Возможные значения: • enabled • disabled
cs4Label	Всегда oldLdapServer.
cs4	Сервер LDAP перед обновлением.
cs5Label	Всегда newLdapServer.
cs5	Сервер LDAP после обновления.
cs6Label	Всегда oldLdapPort.
cs6	Номер порта сервера LDAP перед обновлением.
cs7Label	Всегда newLdapPort.
cs7	Номер порта сервера LDAP после обновления.
cs8Label	Всегда oldConnectionType.

Ключ	Значение
cs8	Тип подключения перед обновлением. Возможные значения: • none • sslTls • starttls
cs9Label	Всегда newConnectionType.
cs9	Тип подключения после обновления. Возможные значения: • none • sslTls • starttls
cs10Label	Всегда oldDomainController.
cs10	Контроллер домена перед обновлением.
cs11Label	Всегда newDomainController.
cs11	Контроллер домена после обновления.
cs12Label	Всегда oldAccountFormat.
cs12	Формат учетной записи перед обновлением. Возможные значения: • userPrincipalName • sAMAccountName
cs13Label	Всегда newAccountFormat.
cs13	Формат учетной записи после обновления. Возможные значения: • userPrincipalName • AMAccountName
cs14Label	Всегда adminFilterChanged. Ключ присутствует, только если правила фильтрации для учетных записей администраторов были изменены.
cs14	true, если правила фильтрации для учетных записей администраторов были изменены. В противном случае ключ отсутствует.
cs15Label	Всегда analystFilterChanged. Ключ присутствует, только если правила фильтрации для учетных записей аналитиков были изменены.
cs15	true, если правила фильтрации для учетных записей аналитиков были изменены. В противном случае ключ отсутствует.
cs16Label	Всегда tenantFilteringRulesChanged. Ключ присутствует, только если правила фильтрации для тенантов были изменены.
cs16	true, если правила фильтрации для тенантов были изменены. В противном случае ключ отсутствует.

События типа EPS Settings Updated

События действий пользователей типа EPS Settings Updated имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
cs2Label	Всегда systemEPSlimitStatus.
cs2	Указывает, включен ли пороговый EPS системы. Возможные значения: • enabled • disabled
cs3Label	Всегда oldSystemEPSlimit.
cs3	Пороговый EPS системы перед обновлением.
cs4Label	Всегда newSystemEPSlimit.
cs4	Пороговый EPS системы после обновления.

События типа Service Alerts Settings Updated

События действий пользователей типа Service Alerts Settings Updated имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
cs2Label	Всегда alertsStatus.
cs2	Признак включенной или выключенной отправки служебных оповещений. Возможные значения: • enabled • disabled
cs3Label	Всегда oldHost.
cs3	IP-адрес или имя хоста перед обновлением.
cs4Label	Всегда newHost.
cs4	IP-адрес или имя хоста после обновления.
cs5Label	Всегда oldPort.
cs5	Номер порта перед обновлением.
cs6Label	Всегда newPort.
cs6	Номер порта после обновлений.
cs7Label	Всегда oldSecureConnection.
cs7	Тип безопасного подключения перед обновлением. Возможные значения: • none • tlsWithCertificateValidation • tlsWithoutCertificateValidation
cs8Label	Всегда newSecureConnection.
cs8	Тип безопасного подключения после обновления. Возможные значения: • none • tlsWithCertificateValidation • tlsWithoutCertificateValidation

События типа `Service Alerts Format Updated`

События действий пользователей типа `Service Alerts Format Updated` имеют уровень критичности `Low`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `oldAlertFormat`.
`cs2`	Формат служебных оповещений перед обновлением.
`cs3Label`	Всегда `newAlertFormat`.
`cs3`	Формат служебных оповещений после обновления.
`cs4Label`	Всегда `oldContextFormat`.
`cs4`	Формат контекста записей перед обновлением.
`cs5Label`	Всегда `newContextFormat`.
`cs5`	Формат контекста записей после обновления.

События типа `Web Interface Settings Updated`

События действий пользователей типа `Web Interface Settings Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `oldHost`.
`cs2`	IP-адрес или имя хоста веб-интерфейса перед обновлением.
`cs3Label`	Всегда `newHost`.
`cs3`	IP-адрес или имя хоста веб-интерфейса после обновления.

События типа `Proxy Settings Updated`

События действий пользователей типа `Proxy Settings Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `oldStatus`.
`cs2`	Статус прокси перед обновлением. Возможные значения: • `enabled` • `disabled`

Ключ	Значение
cs3Label	Всегда newStatus.
cs3	Статус прокси после обновления. Возможные значения: • enabled • disabled
cs4Label	Всегда oldProxyHost.
cs4	IP-адрес или имя хоста прокси-сервера перед обновлением.
cs5Label	Всегда newProxyHost.
cs5	IP-адрес или имя хоста прокси-сервера после обновления.
cs6Label	Всегда oldProxyPort.
cs6	Номер порта прокси-сервера перед обновлением.
cs7Label	Всегда newProxyPort.
cs7	Номер порта прокси-сервера после обновления.
cs8Label	Всегда oldCredentialsStatus.
cs8	Указывает, использовались ли учетные данные для прокси-сервера перед обновлением. Возможные значения: • enabled • disabled
cs9Label	Всегда newCredentialsStatus.
cs9	Указывает, использовались ли учетные данные для прокси-сервера после обновления. Возможные значения: • enabled • disabled
cs10Label	Всегда proxyUsernameChanged. Ключ присутствует, только если имя пользователя для прокси-сервера было изменено.
cs10	true, если имя пользователя прокси-сервера было изменено. В противном случае ключ отсутствует.
cs11Label	Всегда proxyPasswordChanged. Ключ присутствует, только если для прокси-сервера был изменен пароль.
cs11	true, если пароль прокси-сервера был изменен. В противном случае ключ отсутствует.

События типа Audit Settings Updated

События действий пользователей типа Audit Settings Updated имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
cs2Label	Всегда sendingStatus.
cs2	Указывает, отправляются ли события аудита в другие программы. Возможные значения: • enabled • disabled
cs3Label	Всегда oldHost.

Ключ	Значение
`cs3`	IP-адрес или имя хоста перед обновлением.
`cs4Label`	Всегда `newHost`.
`cs4`	IP-адрес или имя хоста после обновления.
`cs5Label`	Всегда `oldPort`.
`cs5`	Номер порта перед обновлением.
`cs6Label`	Всегда `newPort`.
`cs6`	Номер порта после обновления.
`cs7Label`	Всегда `oldSecureConnection`.
`cs7`	Тип безопасного подключения перед обновлением. Возможные значения: • `none` • `tlsWithCertificateValidation` • `tlsWithoutCertificateValidation`
`cs8Label`	Всегда `newSecureConnection`.
`cs8`	Тип безопасного подключения после обновления. Возможные значения: • `none` • `tlsWithCertificateValidation` • `tlsWithoutCertificateValidation`
`cs9Label`	Всегда `oldRetentionDays`.
`cs9`	Срок хранения событий аудита перед обновлением (в днях). Если срок хранения не ограничен, значение `disabled`.
`cs10Label`	Всегда `newRetentionDays`.
`cs10`	Срок хранения событий аудита после обновления (в днях). Если срок хранения не ограничен, значение `disabled`.

События типа `KSN Statement Status Updated`

События действий пользователей типа `KSN Statement Status Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `ksnStatementStatus`.
`cs2`	Статус принятия Положения KSN после обновления. Возможные значения: • `accepted` • `rejected`

События типа `Logging Settings Updated`

События действий пользователей типа `Logging Settings Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключ	Значение
`cs2Label`	Всегда `oldLoggingType`.
`cs2`	Тип журналов перед обновлением. Возможные значения: • `basic` • `syslog`
`cs3Label`	Всегда `newLoggingType`.
`cs3`	Тип журнала после обновления. Возможные значения: • `basic` • `syslog`
`cs4Label`	Всегда `oldLoggingLevel`.
`cs4`	Уровень ведения журнала перед обновлением. Возможные значения: • `non` • `err` • `inf` • `dbg` • `any`
`cs5Label`	Всегда `newLoggingLevel`.
`cs5`	Уровень ведения журнала после обновления. Возможные значения: • `non` • `err` • `inf` • `dbg` • `any`
`cs6Label`	Всегда `oldAutoDeleteStatus`.
`cs6`	Указывает, было ли включено автоматическое удаление старых файлов журнала перед обновлением. Возможные значения: • `enabled` • `disabled`
`cs7Label`	Всегда `newAutoDeleteStatus`.
`cs7`	Указывает, включено ли автоматическое удаление старых файлов журнала после обновления. Возможные значения: • `enabled` • `disabled`
`cs8Label`	Всегда `oldMaxFileSize`.
`cs8`	Максимальный размер одного файла журнала перед обновлением.
`cs9Label`	Всегда `newMaxFileSize`.
`cs9`	Максимальный размер одного файла журнала после обновления.
`cs10Label`	Всегда `oldMaxTotalSize`.
`cs10`	Максимальный общий размер всех файлов журнала перед обновлением. Если общий размер не был ограничен, значение `disabled`.
`cs11Label`	Всегда `newMaxTotalSize`.
`cs11`	Максимальный общий размер всех файлов журнала после обновления. Если общий размер не ограничен, значение `disabled`.

События типа `Detection Storage Settings Updated`

События действий пользователей типа `Detection Storage Settings Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `oldStorageStatus`.
`cs2`	Указывает, было ли включено сохранение обнаружений киберугроз перед обновлением. Возможные значения: • `enabled` • `disabled`
`cs3Label`	Всегда `newStorageStatus`.
`cs3`	Указывает, включено ли сохранение обнаружений киберугроз после обновления. Возможные значения: • `enabled` • `disabled`
`cs4Label`	Всегда `oldMaxStorageSize`.
`cs4`	Максимальный размер хранимых обнаружений киберугроз перед обновлением (в гигабайтах). Если размер не ограничен, значения `disabled`.
`cs5Label`	Всегда `newMaxStorageSize`.
`cs5`	Максимальный размер хранимых обнаружений киберугроз после обновления (в гигабайтах). Если размер не ограничен, значения `disabled`.

События типа `Detection Storage Cleared`

События действий пользователей типа `Detection Storage Cleared` имеют уровень критичности `Medium`. Расширения событий этого типа включают только общие ключи и значения.

Класс событий License

Помимо общих ключей и значений, события действий пользователей, принадлежащие классу `License`, содержат разные ключи и значения, зависящие от типа события.

События типа `License Key Added`

События действий пользователей типа `License Key Added` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `licenseType`.
`cs2`	Тип добавляемого лицензионного ключа. Возможные значения: • `activationCode` • `keyFile`
`cs3Label`	Всегда `licenseLevel`.

Ключ	Значение
cs3	Уровень лицензирования добавленного лицензионного ключа.
cs4Label	Всегда expirationDate.
cs4	Дата и время истечения срока действия лицензионного ключа (UTC) в формате ISO 8601.

События типа Active License Key Deleted

События действий пользователей типа Active License Key Deleted имеют уровень критичности High. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
cs2Label	Всегда licenseLevel.
cs2	Уровень лицензирования удаленного лицензионного ключа.

Класс событий ServiceFeeds

Помимо общих ключей и значений, события действий пользователей, принадлежащие классу ServiceFeeds, содержат разные ключи и значения, зависящие от типа события.

События типа Feed Update Frequency Updated

События действий пользователей с типом Feed Update Frequency Updated имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
cs2Label	Всегда oldUpdateFrequency.
cs2	Частота обновления потоков данных перед обновлением (в минутах).
cs3Label	Всегда newUpdateFrequency.
cs3	Частота обновления потоков данных после обновления (в минутах).

События типа Custom Feed Added

События действий пользователей типа Custom Feed Added имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
cs2Label	Всегда feedName.
cs2	Название пользовательского потока данных.
cs3Label	Всегда feedType.
cs3	Тип пользовательского потока данных. Возможные значения: • csv • json • STIX • xml • misp • pdf • email

Ключ	Значение
`cs4Label`	Всегда `vendorName`.
`cs4`	Название производителя пользовательского потока данных.
`cs5Label`	Всегда `confidenceLevel`.
`cs5`	Уровень доверенности пользовательского потока данных (от 0 до 100).
`cs6Label`	Всегда `customUpdateFrequencyEnabled`.
`cs6`	Указывает, включена ли индивидуальная частота обновления пользовательского потока данных. Возможные значения: • `enabled` • `disabled`
`cs7Label`	Всегда `customUpdateFrequencyMinutes`.
`cs7`	Индивидуальная частота обновления пользовательского потока данных (в минутах). Если для `cs6` значение `disabled` (пользовательская частота обновления отключена), значение `default`.
`cs8Label`	Всегда `proxyEnabled`.
`cs8`	Указывает, используется ли прокси-сервер для обновления пользовательского потока данных. Возможные значения: • `enabled` • `disabled`

События типа `Service Feed Certificate Imported`

События действий пользователей типа `Service Feed Certificate Imported` имеют уровень критичности `Medium`. Расширения событий этого типа включают только общие ключи и значения.

События типа `Service Feed Enabled`

События действий пользователей типа `Service Feed Enabled` имеют уровень критичности `Medium`. События этого типа регистрируются в режиме **Управление системой**. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `feedName`.
`cs2`	Имя потока данных об угрозах.
`cs3Label`	Всегда `vendorName`.
`cs3`	Имя поставщика потока данных.

События типа `Service Feed Disabled`

События действий пользователей типа `Service Feed Disabled` имеют уровень критичности `Medium`. События этого типа регистрируются в режиме **Управление системой**. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `feedName`.
`cs2`	Имя потока данных об угрозах.

Ключ	Значение
cs3Label	Всегда vendorName.
cs3	Имя поставщика потока данных.

События типа Proxy for Kaspersky Threat Data Feeds Updated

События действий пользователей типа Proxy for Kaspersky Threat Data Feeds Updated имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
cs2Label	Всегда oldProxyStatus.
cs2	Указывает, был ли включен прокси для обновления Kaspersky Threat Data Feeds перед обновлением. Возможные значения: • enabled • disabled
cs3Label	Всегда newProxyStatus.
cs3	Указывает, включен ли прокси для обновления Kaspersky Threat Data Feeds после обновления. Возможные значения: • enabled • disabled

События типа Service Feed Updated

События действий пользователей типа Service Feed Updated имеют уровень критичности Medium. События этого типа регистрируются в режиме **Управление системой**. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
cs2Label	Всегда feedName.
cs2	Имя потока данных об угрозах.
cs3Label	Всегда vendorName.
cs3	Имя поставщика потока данных.
cs4Label	Всегда oldFeedStatus.
cs4	Статус потока данных перед обновлением. Возможные значения: • enabled • disabled
cs5Label	Всегда newFeedStatus.
cs5	Статус потока данных после обновления. Возможные значения: • enabled • disabled

Ключ	Значение
`cs6Label`	Всегда `oldAvailableFields`.
`cs6`	Список полей, доступных в потоке данных перед обновлением, разделенных запятыми.
`cs7Label`	Всегда `newAvailableFields`.
`cs7`	Список полей, доступных в потоке данных после обновления, разделенных запятыми.
`cs8Label`	Всегда `oldConfidenceLevel`.
`cs8`	Уровень доверенности потока данных перед обновлением (от 0 до 100).
`cs9Label`	Всегда `newConfidenceLevel`.
`cs9`	Уровень доверенности потока данных после обновления (от 0 до 100).
`cs10Label`	Всегда `oldTruncateStatus`.
`cs10`	Указывает, было ли включено сокращение потока данных перед обновлением. Возможные значения: • `enabled` • `disabled`
`cs11Label`	Всегда `newTruncateStatus` .
`cs11`	Указывает, включено ли сокращение потока данных после обновления. Возможные значения: • `enabled` • `disabled`
`cs12Label`	Всегда `oldMaxRecords`.
`cs12`	Максимальное количество записей перед обновлением, если поток данных сокращен. Если поток данных не сокращен после изменений, значение `disabled`.
`cs13Label`	Всегда `newMaxRecords`.
`cs13`	Максимальное количество записей после обновления, если поток данных сокращен.
`cs14Label`	Всегда `oldRetentionStatus`.
`cs14`	Указывает, было ли включено сохранение потока данных перед обновлением. Возможные значения: • `enabled` • `disabled`
`cs15Label`	Всегда `newRetentionStatus`.
`cs15`	Указывает, включено ли сохранение потока данных после обновления. Возможные значения: • `enabled` • `disabled`
`cs16Label`	Всегда `oldRetentionAmount`.
`cs16`	Срок хранения перед обновлением в минутах. Если хранение было отключено, значение `disabled`.
`cs17Label`	Всегда `newRetentionAmount`.
`cs17`	Срок хранения после обновления в минутах.
`cs18Label`	Всегда `filteringRulesChanged`.
`cs18`	Изменение правил фильтрации. Возможные значения: • `added` • `removed`

События типа `Service Feed Settings Updated`

События действий пользователей типа `Service Feed Settings Updated` имеют уровень критичности `Medium`. События этого типа регистрируются в режиме **Управление системой**. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `feedName`.
`cs2`	Имя потока данных об угрозах.
`cs3Label`	Всегда `oldFeedName`.
`cs3`	Имя потока данных перед обновлением.
`cs4Label`	Всегда `newFeedName`.
`cs4`	Имя потока данных после обновления.
`cs5Label`	Всегда `oldVendorName`.
`cs5`	Имя поставщика потока данных перед обновлением.
`cs6Label`	Всегда `newVendorName`.
`cs6`	Имя поставщика потока данных после обновления.
`cs7Label`	Всегда `oldConfidenceLevel`.
`cs7`	Уровень доверенности потока данных перед обновлением (от 0 до 100).
`cs8Label`	Всегда `newConfidenceLevel`.
`cs8`	Уровень доверенности потока данных после обновления (от 0 до 100).
`cs9Label`	Всегда `feedPathChanged`. Ключ присутствует, только если путь к потоку данных был изменен.
`cs9`	`true`, если путь к потоку данных был изменен. В противном случае ключ отсутствует.
`cs10Label`	Всегда `oldUpdateFrequency`.
`cs10`	Частота обновления потоков данных перед обновлением (в минутах). Если поток данных унаследовал частоту обновления по умолчанию, значение `default`.
`cs11Label`	Всегда `newUpdateFrequency`.
`cs11`	Частота обновления потоков данных после обновления (в минутах). Если поток данных наследует частоту обновления по умолчанию, значение `default`.
`cs12Label`	Всегда `oldProxyStatus`.
`cs12`	Указывает, использовался ли прокси для обновления потока данных перед обновлением. Возможные значения: • `enabled` • `disabled`
`cs13Label`	Всегда `newProxyStatus`.
`cs13`	Указывает, используется ли прокси для обновления потока данных после обновления. Возможные значения: • `enabled` • `disabled`

События типа `Service Feed Deleted`

События действий пользователей типа `Service Feed Deleted` имеют уровень критичности `Medium`. События этого типа регистрируются в режиме **Управление системой**. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `feedName`.
`cs2`	Имя удаленного потока данных.

Класс событий Tenant

Помимо общих ключей и значений, события действий пользователей, принадлежащие классу `Tenant`, содержат разные ключи и значения, зависящие от типа события.

События типа `Tenant Created`

События действий пользователей с типом `Tenant Created` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `createTenantName`.
`cs2`	Имя созданного тенанта.
`cs3Label`	Всегда `tenantDescription`.
`cs3`	Описание созданного тенанта.
`cs4Label`	Всегда `siem`.
`cs4`	SIEM-система, выбранная для тенанта.
`cs5Label`	Всегда `epsLimitStatus`.
`cs5`	Указывает, включен ли пороговый EPS для тенанта. Возможные значения: • `enabled` • `disabled`
`cs6Label`	Всегда `epsLimitValue`.
`cs6`	Пороговый EPS для тенанта. Если пороговый EPS отключен, значение `disabled`.
`cs7Label`	Всегда `ip`. Если в качестве типа подключения для созданного тенанта был выбран сокет UNIX, этот ключ отсутствует.
`cs7`	IP-адрес входящих событий. Если в качестве типа подключения для созданного тенанта был выбран сокет UNIX, этот ключ отсутствует.
`cs8Label`	Всегда `port`. Если в качестве типа подключения для созданного тенанта был выбран сокет UNIX, этот ключ отсутствует.
`cs8`	Номер порта входящих событий. Если в качестве типа подключения для созданного тенанта был выбран сокет UNIX, этот ключ отсутствует.
`cs9Label`	Всегда `unixSocket`. Если в качестве типа подключения для созданного тенанта были выбраны IP-адрес и порт, этот ключ отсутствует.
`cs9`	Сокет UNIX входящих событий. Если в качестве типа подключения для созданного тенанта были выбраны IP-адрес и порт, этот ключ отсутствует.

Ключ	Значение
cs10Label	Всегда secureIncomingConnection. Если в качестве типа подключения для созданного тенанта был выбран сокет UNIX, этот ключ отсутствует.
cs10	Тип защищенного входящего подключения. Возможные значения: • none • tls Если в качестве типа подключения для созданного тенанта был выбран сокет UNIX, этот ключ отсутствует.
cs11Label	Всегда Host.
cs11	IP-адрес или имя хоста для оповещений об обнаружении индикаторов компрометации.
cs12Label	Всегда port.
cs12	Номер порта для оповещений об обнаружении индикаторов компрометации.
cs13Label	Всегда secureOutgoingConnection.
cs13	Тип безопасного исходящего подключения. Возможные значения: • none • tlsWithCertificateValidation • tlsWithoutCertificateValidation

События типа Tenant Deleted

События действий пользователей с типом Tenant Deleted имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
cs2Label	Всегда deleteTenantName.
cs2	Имя удаленного тенанта.

События типа Tenant Basic Settings Updated

События действий пользователей типа Tenant Basic Settings Updated имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
cs2Label	Всегда oldTenantName.
cs2	Имя тенанта перед обновлением.
cs3Label	Всегда newTenantName.
cs3	Имя тенанта после обновления.
cs4Label	Всегда oldTenantDescription.
cs4	Описание тенанта перед обновлением.
cs5Label	Всегда newTenantDescription.
cs5	Описание тенанта после обновления.

События типа `Tenant EPS Settings Updated`

События действий пользователей типа `Tenant EPS Settings Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `oldEPSLimitStatus`.
`cs2`	Указывает, был ли включен пороговый EPS для тенанта перед обновлением. Возможные значения: • `enabled` • `disabled`
`cs3Label`	Всегда `newEPSLimitStatus`.
`cs3`	Указывает, включен ли пороговый EPS для тенанта после обновления. Возможные значения: • `enabled` • `disabled`
`cs4Label`	Всегда `oldEPSLimitValue`.
`cs4`	Пороговый EPS для тенанта перед обновлением. Если пороговый EPS был отключен, значение `disabled`.
`cs5Label`	Всегда `newEPSLimitValue`.
`cs5`	Пороговый EPS для тенанта после обновления. Если пороговый EPS отключен, значение `disabled`.

События типа `Settings for Tenant Incoming Events Updated`

События действий пользователей типа `Settings for Tenant Incoming Events Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `oldHost`. Если в качестве типа подключения для тенанта был выбран сокет UNIX, этот ключ отсутствует.
`cs2`	IP-адрес входящих событий перед обновлением. Если в качестве типа подключения для тенанта был выбран сокет UNIX, этот ключ отсутствует.
`cs3Label`	Всегда `newHost`. Если в качестве типа подключения для тенанта был выбран сокет UNIX, этот ключ отсутствует.
`cs3`	IP-адрес входящих событий после обновления. Если в качестве типа подключения для тенанта был выбран сокет UNIX, этот ключ отсутствует.
`cs4Label`	Всегда `oldPort`. Если в качестве типа подключения для тенанта был выбран сокет UNIX, этот ключ отсутствует.

Ключ	Значение
`cs4`	Порт входящих событий перед обновлением. Если в качестве типа подключения для тенанта был выбран сокет UNIX, этот ключ отсутствует.
`cs5Label`	Всегда `newPort`. Если в качестве типа подключения для тенанта был выбран сокет UNIX, этот ключ отсутствует.
`cs5`	Порт входящих событий после обновления. Если в качестве типа подключения для тенанта был выбран сокет UNIX, этот ключ отсутствует.
`cs6Label`	Всегда `oldUnixSocketPath`. Если в качестве типа подключения для тенанта были выбраны IP-адрес и порт, этот ключ отсутствует.
`cs6`	Путь к сокету UNIX входящих событий перед обновлением. Если в качестве типа подключения для тенанта были выбраны IP-адрес и порт, этот ключ отсутствует.
`cs7Label`	Всегда `newUnixSocketPath`. Если в качестве типа подключения для тенанта были выбраны IP-адрес и порт, этот ключ отсутствует.
`cs7`	Путь к сокету UNIX входящих событий после обновления. Если в качестве типа подключения для тенанта были выбраны IP-адрес и порт, этот ключ отсутствует.
`cs8Label`	Всегда `oldSecureConnection`.
`cs8`	Тип безопасного подключения для входящих событий перед обновлением. Возможные значения: • `none` • `tls`
`cs9Label`	Всегда `newSecureConnection`.
`cs9`	Тип безопасного подключения для входящих событий после обновления. Возможные значения: • `none` • `tls`

События типа `Settings for Tenant Detection Alerts Updated`

События действий пользователей типа `Settings for Tenant Detection Alerts Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `oldHost`.
`cs2`	IP-адрес или имя хоста для оповещений об обнаружении индикаторов компрометации перед обновлением.
`cs3Label`	Всегда `newHost`.
`cs3`	IP-адрес или имя хоста для оповещений об обнаружении индикаторов компрометации после обновления.
`cs4Label`	Всегда `oldPort`.
`cs4`	Порт оповещений об обнаружении индикаторов компрометации перед обновлением.
`cs5Label`	Всегда `newPort`.
`cs5`	Порт оповещений об обнаружении индикаторов компрометации после обновления.
`cs6Label`	Всегда `oldSecureConnection`.

Ключ	Значение
cs6	Тип безопасного подключения для оповещений об обнаружении индикаторов компрометации перед обновлением. Возможные значения: • none • tls
cs7Label	Всегда newSecureConnection.
cs7	Тип безопасного подключения для оповещений об обнаружении индикаторов компрометации после изменений. Возможные значения: • none • tls

События типа Settings for Tenant Service Events Updated

События действий пользователей типа Settings for Tenant Service Events Updated имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
cs2Label	Всегда oldServiceEventsStatus.
cs2	Указывает, была ли включена отправка событий тенанта службы перед обновлением. Возможные значения: • enabled • disabled
cs3Label	Всегда newServiceEventsStatus.
cs3	Указывает, включена ли отправка событий тенанта службы после обновления. Возможные значения: • enabled • disabled
cs4Label	Всегда oldHost.
cs4	IP-адрес или хост для отправки событий тенанта службы перед обновлением.
cs5Label	Всегда newHost.
cs5	IP-адрес или хост для отправки событий тенанта службы после обновления.
cs6Label	Всегда oldPort.
cs6	Порт для отправки событий тенанта службы перед обновлением.
cs7Label	Всегда newPort.
cs7	Порт для отправки событий тенанта службы после обновления.
cs8Label	Всегда oldSecureConnection.
cs8	Тип безопасного подключения для отправки событий тенанта службы перед обновлением. Возможные значения: • none • tlsWithCertificateValidation • tlsWithoutCertificateValidation
cs9Label	Всегда newSecureConnection.

Ключ	Значение
cs9	Тип безопасного подключения для отправки событий тенанта службы после обновления. Возможные значения: • none • tlsWithCertificateValidation • tlsWithoutCertificateValidation

События типа Settings for Tenant API Lookup Detections Updated

События действий пользователей типа Settings for Tenant API Lookup Detections Updated имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
cs2Label	Всегда newLookupDetectionsStatus.
cs2	Указывает, включена ли отправка обнаружений с помощью API lookup после обновления. Возможные значения: • enabled • disabled

События типа Tenant Statistics Reset

События действий пользователей с типом Tenant Statistics Reset имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
cs2Label	Всегда statisticsResetTenantName.
cs2	Имя тенанта, для которого была сброшена статистика.

Класс событий TenantSettings

Помимо общих ключей и значений, события действий пользователей, принадлежащие классу TenantSettings, содержат разные ключи и значения, зависящие от типа события.

События типа Tenant Event Source Created

События действий пользователей с типом Tenant Event Source Created имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
cs2Label	Всегда sourceID.
cs2	Идентификатор созданного источника событий.
cs3Label	Всегда sourceType.
cs3	Тип созданного источника событий. Возможные значения: • ipAddress • hostName • regularExpression
cs4Label	Всегда sourceValue.

Ключ	Значение
cs4	Значение источника событий.
cs5Label	Всегда replacementRulesUsed.
cs5	Указывает, применяются ли правила замены к событиям из созданного источника. Возможные значения: • enabled • disabled
cs6Label	Всегда ReplacementRulesCount.
cs6	Число правил замены. Если правила замены не используются, значение 0.
cs7Label	Всегда ignoreRulesUsed.
cs7	Указывает, применяются ли правила игнорирования к событиям из созданного источника. Возможные значения: • enabled • disabled
cs8Label	Всегда ignoreRulesCount.
cs8	Количество правил игнорирования. Если правила игнорирования не применяются, значение 0.
cs9Label	Всегда regularExpressionsCount.
cs9	Число регулярных выражений.

События типа Normalization Rules of Tenant Event Source Updated

События действий пользователей с типом Normalization Rules of Tenant Event Source Updated имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
cs2Label	Всегда sourceID.
cs2	Идентификатор источника событий, для которого были обновлены правила нормализации.
cs3Label	Всегда oldReplacementRulesCount.
cs3	Общее число правил замены перед обновлением.
cs4Label	Всегда newReplacementRulesCount.
cs4	Общее число правил замены после обновления.
cs5Label	Всегда oldIgnoreRulesCount.
cs5	Общее число правил игнорирования перед обновлением.
cs6Label	Всегда newIgnoreRulesCount.
cs6	Общее число правил игнорирования после обновления.

События типа `Regular Expressions of Tenant Event Source Updated`

События действий пользователей с типом `Regular Expressions of Tenant Event Source Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `sourceID`.
`cs2`	Идентификатор источника событий, для которого были обновлены регулярные выражения.
`cs3Label`	Всегда `oldRegularExpressionsCount`.
`cs3`	Общее число регулярных выражений перед обновлением.
`cs4Label`	Всегда `newRegularExpressionsCount`.
`cs4`	Общее число регулярных выражений после обновления.

События типа `Tenant Event Source Deleted`

События действий пользователей с типом `Tenant Event Source Deleted` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `sourceID`.
`cs2`	Идентификатор удаленного источника событий.
`cs3Label`	Всегда `sourceType`.
`cs3`	Тип удаленного источника событий. Возможные значения: • `ipAddress` • `hostName` • `regularExpression`
`cs4Label`	Всегда `sourceValue`.
`cs4`	Значение источника событий.

События типа `Format of Tenant Service Alerts Updated`

События действий пользователей типа `Format of Tenant Service Alerts Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
cs2Label	Всегда oldAlertFormat.
cs2	Формат служебных оповещений перед обновлением.
cs3Label	Всегда newAlertFormat.
cs3	Формат служебных оповещений после обновления.
cs4Label	Всегда oldContextFormat.
cs4	Формат контекста служебного оповещения перед обновлением.
cs5Label	Всегда newContextFormat.
cs5	Формат контекста служебного оповещения после обновления.

События типа Format of Tenant Detection Alerts Updated

События действий пользователей типа Format of Tenant Detection Alerts Updated имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
cs2Label	Всегда oldAlertFormat.
cs2	Формат оповещения об обнаружении индикаторов компрометации перед обновлением.
cs3Label	Всегда newAlertFormat.
cs3	Формат оповещения об обнаружении индикаторов компрометации после обновления.

События типа Filtering of Tenant Detection Alerts Updated

События действий пользователей типа Filtering of Tenant Detection Alerts Updated имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
cs2Label	Всегда oldFilteringRulesCount.
cs2	Общее число правил фильтрации перед обновлением.
cs3Label	Всегда newFilteringRulesCount.
cs3	Общее число правил фильтрации после обновления.

События типа Context of Tenant Detection Alerts Updated

События действий пользователей типа Context of Tenant Detection Alerts Updated имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
cs2Label	Всегда oldContextFormat.
cs2	Формат контекста оповещений об обнаружении индикаторов компрометации тенанта перед обновлением.
cs3Label	Всегда newContextFormat.
cs3	Формат контекста оповещений об обнаружении индикаторов компрометации тенанта после обновления.

Класс событий TenantFeeds

Помимо общих ключей и значений, события действий пользователей, принадлежащие классу `TenantFeeds`, содержат разные ключи и значения, зависящие от типа события.

События типа `Tenant Feed Enabled`

События действий пользователей типа `Tenant Feed Enabled` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `feedName`.
`cs2`	Название включенного потока данных.
`cs3Label`	Всегда `vendorName`.
`cs3`	Название производителя включенного потока данных.

События типа `Tenant Feed Disabled`

События действий пользователей типа `Tenant Feed Disabled` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `feedName`.
`cs2`	Имя отключенного потока данных.
`cs3Label`	Всегда `vendorName`.
`cs3`	Название производителя отключенного потока данных.

События типа `FalsePositive List Updated`

События действий пользователей типа `FalsePositive List Updated` имеют уровень критичности `Medium`. Расширения событий этого типа включают только общие ключи и значения.

События типа `InternalTI List Updated`

События действий пользователей типа `InternalTI List Updated` имеют уровень критичности `Medium`. Расширения событий этого типа включают только общие ключи и значения.

Класс событий TenantIndicators

Помимо общих ключей и значений, события действий пользователей, принадлежащие классу `TenantIndicators`, содержат разные ключи и значения, зависящие от типа события.

События типа `Indicator Deleted`

События действий пользователей с типом `Indicator Deleted` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `indicatorValue`.
`cs2`	Значение удаленного индикатора.

События типа `Indicator Enriched`

События действий пользователей с типом `Indicator Enriched` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `indicatorValue`.
`cs2`	Значение обогащенного индикатора.
`cs3Label`	Всегда `enrichmentSource`.
`cs3`	Источник обогащения.

События типа `Indicator Publications Queried`

События действий пользователей с типом `Indicator Publications Queried` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `publicationId`.
`cs2`	Идентификатор запрашиваемой публикации.
`cs3Label`	Всегда `publicationsSource`.
`cs3`	Источник публикации, на которую был отправлен запрос.
`cs4Label`	Всегда `publicationType`.
`cs4`	Тип запрашиваемой публикации. Возможные значения: • `all` • `pdf` • `summary` • `yara` • `iocs` • `suricata`

События типа `Indicator Tags Updated`

События действий пользователей с типом `Indicator Tags Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `indicatorValue`.
`cs2`	Значение индикатора, для которого обновлялись теги.

Класс событий RetroScan

Помимо общих ключей и значений, события действий пользователей, принадлежащие классу `RetroScan`, содержат разные ключи и значения, зависящие от типа события.

События типа `RetroScan Started`

События действий пользователей с типом `RetroScan Started` имеют уровень критичности `Medium`. События этого типа регистрируются при запуске ретроспективного сканирования вручную. Расширения событий этого типа включают только общие ключи и значения.

События типа `RetroScan Events Cleared`

События действий пользователей типа `RetroScan Events Cleared` имеют уровень критичности `Medium`. Расширения событий этого типа включают только общие ключи и значения.

События типа `RetroScan Status Updated`

События действий пользователей типа `RetroScan Status Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `newStatus`.
`cs2`	Указывает, включен ли ретроскан. Возможные значения: • `enabled` • `disabled`

События типа `RetroScan Settings Updated`

События действий пользователей типа `RetroScan Settings Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `oldFrequency`.
`cs2`	Частота ретроскана перед обновлением. Возможные значения: • `everyDay` • `everyWeek` • `everyTwoWeeks` • `everyMonth`
`cs3Label`	Всегда `newFrequency`.
`cs3`	Частота ретроскана после обновления. Возможные значения: • `everyDay` • `everyWeek` • `everyTwoWeeks` • `everyMonth`

Ключ	Значение
cs4Label	Всегда oldRetentionEventsDays.
cs4	Срок хранения событий ретроскана перед обновлением (в днях).
cs5Label	Всегда newRetentionEventsDays.
cs5	Срок хранения событий ретроскана после обновления (в днях).
cs6Label	Всегда oldRetentionResultsDays.
cs6	Срок хранения результатов ретроскана перед обновлением (в днях).
cs7Label	Всегда newRetentionResultsDays.
cs7	Срок хранения результатов ретроскана после обновления (в днях).
cs8Label	Всегда oldMaxSizeGB.
cs8	Максимальный размер хранимых событий ретроскана перед обновлением (в гигабайтах). Если размер не был ограничен, значение disabled.
cs9Label	Всегда newMaxSizeGB.
cs9	Максимальный размер хранимых событий ретроскана после обновления (в гигабайтах). Если размер не ограничен, значение disabled.

События типа RetroScan Feeds Updated

События действий пользователей типа RetroScan Feeds Updated имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
cs2Label	Всегда oldEnabledFeedsCount.
cs2	Общее число включенных потоков данных ретроскана перед обновлением.
cs3Label	Всегда newEnabledFeedsCount.
cs3	Общее число включенных потоков данных ретроскана после обновления.

События типа RetroScan Regular Expressions Updated

События действий пользователей типа RetroScan Regular Expressions Updated имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
cs2Label	Всегда retroscanTenant.
cs2	Имя тенанта, для которого были обновлены регулярные выражения.
cs3Label	Всегда sourceName.
cs3	Имя источника событий, для которого были обновлены регулярные выражения.
cs4Label	Всегда oldRegularExpressions.
cs4	Список регулярных выражений, используемых в ретроскане перед обновлением, разделенных запятыми.
cs5Label	Всегда newRegularExpressions.
cs5	Список регулярных выражений, используемых в ретроскане после обновления, разделенных запятыми.

Класс событий ExternalSources

Помимо общих ключей и значений, события действий пользователей, принадлежащие классу `ExternalSources`, содержат разные ключи и значения, зависящие от типа события.

События типа `External Source Created`

События действий пользователей с типом `External Source Created` имеют уровень критичности `Low`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `accessName`.
`cs2`	Имя созданного доступа.
`cs3Label`	Всегда `sourceName`.
`cs3`	Имя внешнего источника, для которого создан доступ.
`cs4Label`	Всегда `assignedTenants`.
`cs4`	Список тенантов, которым назначен доступ, разделенных запятыми.

События типа `External Source Updated`

События действий пользователей с типом `External Source Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `accessName`.
`cs2`	Имя доступа.
`cs3Label`	Всегда `oldAccessName`.
`cs3`	Имя доступа перед обновлением.
`cs4Label`	Всегда `newAccessName`.
`cs4`	Имя доступа после обновления.
`cs5Label`	Всегда `oldAssignedTenants`.
`cs5`	Список тенантов, которым был назначен доступ перед обновлением, разделенных запятыми.
`cs6Label`	Всегда `newAssignedTenants`.
`cs6`	Список тенантов, которым назначен доступ после обновления, разделенных запятыми.
`cs7Label`	Всегда `tokenChanged`. Ключ присутствует, только если токен доступа был изменен.
`cs7`	`true`, если токен доступа был изменен. В противном случае ключ отсутствует.

События типа `External Source Deleted`

События действий пользователей с типом `External Source Deleted` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `accessName`.
`cs2`	Имя удаленного доступа.
`cs3Label`	Всегда `sourceName`.
`cs3`	Имя внешнего источника, доступ к которому был удален.
`cs4Label`	Всегда `assignedTenants`.
`cs4`	Список тенантов, доступ к которым был удален, разделенных запятыми.

Класс событий IndicatorsExport

Помимо общих ключей и значений, события действий пользователей, принадлежащие классу `IndicatorsExport`, содержат разные ключи и значения, зависящие от типа события.

События типа `Indicators Export Task Created`

События действий пользователей с типом `Indicators Export Task Created` имеют уровень критичности `Low`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `taskName`.
`cs2`	Имя созданной задачи экспорта.
`cs3Label`	Всегда `ngfwType`.
`cs3`	Тип NGFW, выбранный для экспорта. Возможные значения: • `generic_csv` (NGFW не выбран) • `check_point` • `cisco_firewall` • `fortigate` • `palo_alto` • `sophos` • `security_code` • `usergate` • `proxysg`
`cs4Label`	Всегда `maxRecords`.
`cs4`	Максимальное число записей для экспорта.
`cs5Label`	Всегда `exportFrequency`.
`cs5`	Частота экспорта (в минутах).
`cs6Label`	Всегда `filteringRulesCount`.
`cs6`	Общее число правил фильтрации, примененных для задачи экспорта.
`cs7Label`	Всегда `securedAccessEnabled`.
`cs7`	Указывает, требуется ли авторизация для доступа к итоговому файлу экспорта. Возможные значения: • `true` • `false`

События типа `Indicators Export Task Deleted`

События действий пользователей с типом `Indicators Export Task Deleted` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `taskName`.
`cs2`	Имя удаленной задачи экспорта.

События типа `Indicators Export Task Updated`

События действий пользователей с типом `Indicators Export Task Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `taskName`.
`cs2`	Имя обновленной задачи экспорта.
`cs3Label`	Всегда `oldTaskName`.
`cs3`	Имя задачи экспорта перед обновлением.
`cs4Label`	Всегда `newTaskName`.
`cs4`	Имя задачи экспорта после обновления.
`cs5Label`	Всегда `oldNgfwType`.
`cs5`	Тип NGFW, выбранный для экспорта перед обновлением. Возможные значения: • `generic_csv` (NGFW не выбран) • `check_point` • `cisco_firewall` • `fortigate` • `palo_alto` • `sophos` • `security_code` • `usergate` • `proxysg`
`cs6Label`	Всегда `новыйNgfwType`.
`cs6`	Тип NGFW, выбранный для экспорта после обновления. Возможные значения: • `generic_csv` (NGFW не выбран) • `check_point` • `cisco_firewall` • `fortigate` • `palo_alto` • `sophos` • `security_code` • `usergate` • `proxysg`
`cs7Label`	Всегда `oldMaxRecords`.
`cs7`	Максимальное число записей для экспорта перед обновлением.
`cs8Label`	Всегда `newMaxRecords`.
`cs8`	Максимальное число записей для экспорта после обновления.
`cs9Label`	Всегда `oldExportFrequency`.
`cs9`	Частота экспорта перед обновлением.

Ключ	Значение
cs10Label	Всегда newExportFrequency.
cs10	Частота экспорта после изменений.
cs11Label	Всегда oldFilteringRulesCount.
cs11	Общее число правил фильтрации, примененных для задачи экспорта перед обновлением.
cs12Label	Всегда newFilteringRulesCount.
cs12	Общее число правил фильтрации, примененных для задачи экспорта после обновления.
cs13Label	Всегда oldSecuredAccessEnabled.
cs13	Указывает, требовалась ли аутентификация для доступа к итоговому файлу экспорта перед обновлением. Возможные значения: • true • false
cs14Label	Всегда newSecuredAccessEnabled.
cs14	Указывает, требуется ли аутентификация для доступа к итоговому файлу экспорта после обновления. Возможные значения: • true • false

События типа Status of Indicators Export Task Changed

События действий пользователей с типом Status of Indicators Export Task Changed имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
cs2Label	Всегда taskName.
cs2	Имя задачи экспорта, статус которой был изменен.
cs3Label	Всегда newStatus.
cs3	Статус задачи экспорта после изменения. Возможные значения: • enabled • disabled

События типа Indicators Export Task Started

События действий пользователей с типом Indicators Export Task Started имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
cs2Label	Всегда taskName.
cs2	Имя задачи экспорта, запущенной вручную.

Класс событий Reporting

Помимо общих ключей и значений, события действий пользователей, принадлежащие классу Reporting, содержат разные ключи и значения, зависящие от типа события.

События типа `Report Task Created`

События действий пользователей с типом `Report Task Created` имеют уровень критичности `Low`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `taskName`.
`cs2`	Название созданной задачи отчета.
`cs3Label`	Всегда `recipientsCount`.
`cs3`	Общее число получателей отчета.
`cs4Label`	Всегда `schedule`.
`cs4`	Расписание отправки отчета в формате `< частота >,< время >,< временная зона >`, где: • `< частота > – день`, `неделя` или `месяц`. • `< время >` имеет формат `ЧЧ:ММ`.
`cs5Label`	Всегда `dataSource`.
`cs5`	Источник данных отчета. Возможные значения: • `all` • `tcp` • `apiLookup`
`cs6Label`	Всегда `reportPeriod`.
`cs6`	Период, за который данные включаются в отчет. Возможные значения: • `lastDay` • `lastWeek` • `lastMonth`
`cs7Label`	Всегда `assignedTenants`.
`cs7`	Список тенантов, для которых был создан отчет, разделенных запятыми. Если отчет создан для всех тенантов, значение `all`.
`cs8Label`	Всегда `widgets`.
`cs8`	Список виджетов, включенных в отчет, разделенных запятыми. Возможные значения: • `statisticsOverview` • `detectionStatistics` • `topIndicatorsByDetection` • `matchingStatistics` • `supplierStatistics`

События типа `Report Task Deleted`

События действий пользователей с типом `Report Task Deleted` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `taskName`.
`cs2`	Имя удаленной задачи отчета.

События типа `Report Task Updated`

События действий пользователей с типом `Report Task Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

> Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `taskName`.
`cs2`	Имя обновленной задачи отчета.
`cs3Label`	Всегда `oldTaskName`.
`cs3`	Название задачи отчета перед обновлением.
`cs4Label`	Всегда `newTaskName`.
`cs4`	Название задачи отчета после обновления.
`cs5Label`	Всегда `recipientsCountChanged`. Ключ присутствует, только если число получателей отчета было изменено.
`cs5`	`true`, если число получателей отчета изменилось. В противном случае ключ отсутствует.
`cs6Label`	Всегда `emailSubjectChanged`. Ключ присутствует, только если тема сообщения электронной почты была изменена.
`cs6`	`true`, если тема сообщения электронной почты по отправке отчета была изменена. В противном случае ключ отсутствует.
`cs7Label`	Всегда `oldSchedule`.
`cs7`	Расписание отправки отчета до обновления в формате `< частота >,< время >,< временная зона >`, где: • `< частота >` – `день`, `неделя` или `месяц`. • `< время >` имеет формат `ЧЧ:ММ`.
`cs8Label`	Всегда `newSchedule`.
`cs8`	Расписание отправки отчета после обновления в формате `< частота >,< время >,< временная зона >`, где: • `< частота >` – `день`, `неделя` или `месяц`. • `< время >` имеет формат `ЧЧ:ММ`.
`cs9Label`	Всегда `oldDataSource`.
`cs9`	Отчет об источнике данных перед обновлением. Возможные значения: • `all` • `tcp` • `apiLookup`
`cs10Label`	Всегда `newDataSource`.
`cs10`	Отчет об источнике данных после обновления. Возможные значения: • `all` • `tcp` • `apiLookup`
`cs11Label`	Всегда `oldReportPeriod`.
`cs11`	Период, за который данные были включены в отчет перед обновлением. Возможные значения: • `lastDay` • `lastWeek` • `lastMonth`

Ключ	Значение
cs12Label	Всегда newReportPeriod.
cs12	Период, за который данные включаются в отчет после обновления. Возможные значения: • lastDay • lastWeek • lastMonth
cs13Label	Всегда oldAssignedTenants.
cs13	Список тенантов, для которых был создан отчет перед обновлением, разделенных запятыми. Если отчет был создан для всех тенантов, значение all.
cs14Label	Всегда newAssignedTenants.
cs14	Список тенантов, для которых создан отчет после обновления, разделенных запятыми. Если отчет создан для всех тенантов, значение all.
cs15Label	Всегда oldWidgets.
cs15	Список виджетов, включенных в отчет до обновления, разделенных запятыми. Возможные значения: • statisticsOverview • detectionStatistics • topIndicatorsByDetection • matchingStatistics • supplierStatistics
cs16Label	Всегда newWidgets.
cs16	Список виджетов, включенных в отчет после обновления, разделенных запятыми. Возможные значения: • statisticsOverview • detectionStatistics • topIndicatorsByDetection • matchingStatistics • supplierStatistics

События типа Report Task Status Changed

События действий пользователей с типом Report Task Status Changed имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
cs2Label	Всегда taskName.
cs2	Имя задачи отчета, статус которой был изменен.
cs3Label	Всегда oldTaskName.
cs3	Статус задачи отчета после обновления. Возможные значения: • enabled • disabled

События типа Report Task Started

События действий пользователей с типом Report Task Started имеют уровень критичности Medium. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `taskName`.
`cs2`	Имя задачи отчета, запущенной вручную.

События типа `Report Generation Started`

События действий пользователей с типом `Report Generation Started` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `taskName`.
`cs2`	Имя задачи формирования отчета, для которой началось формирование отчета.

События типа `Mail Client Settings Updated`

События действий пользователей типа `Mail Client Settings Updated` имеют уровень критичности `Medium`. В таблице ниже перечислены ключи и значения, относящиеся к этому типу событий.

Для ключей, представляющих старые и новые значения параметров, в событии действий пользователя присутствуют только ключи для параметров, которые были обновлены.

Ключи и значения

Ключ	Значение
`cs2Label`	Всегда `oldStatus`.
`cs2`	Статус почтового клиента перед обновлением. Возможные значения: • `enabled` • `disabled`
`cs3Label`	Всегда `newStatus`.
`cs3`	Статус почтового клиента после обновления. Возможные значения: • `enabled` • `disabled`
`cs4Label`	Всегда `oldSmtpServer`.
`cs4`	Адрес SMTP-сервера перед обновлением.
`cs5Label`	Всегда `newSmtpServer`.
`cs5`	Адрес SMTP-сервера перед обновлением.
`cs6Label`	Всегда `oldSmtpPort`.
`cs6`	Номер порта SMTP перед обновлением.
`cs7Label`	Всегда `newSmtpPort`.
`cs7`	Номер порта SMTP после обновления.
`cs8Label`	Всегда `oldSecureConnection`.

Ключ	Значение
`cs8`	Тип безопасного подключения перед обновлением. Возможные значения: • `none` • `sslTls` • `starttls`
`cs9Label`	Всегда `newSecureConnection`.
`cs9`	Тип безопасного подключения после обновления. Возможные значения: • `none` • `sslTls` • `starttls`
`cs10Label`	Всегда `loginChanged`. Ключ присутствует, только если имя учетной записи для почтового клиента было изменено.
`cs10`	`true`, если имя учетной записи почтового клиента было изменено. В противном случае ключ отсутствует.
`cs11Label`	Всегда `emailChanged`. Ключ присутствует, только если адрес электронной почты для почтового клиента был изменен.
`cs11`	`true`, если адрес электронной почты почтового клиента был изменен. В противном случае ключ отсутствует.
`cs12Label`	Всегда `passwordChanged`. Ключ присутствует, только если пароль для почтового клиента был изменен.
`cs12`	`true`, если пароль почтового клиента был изменен. В противном случае ключ отсутствует.

Настройка журналов

Управлять общими параметрами ведения журналов можно в веб-интерфейсе Kaspersky CyberTrace на странице **Параметры** → **Журналы**. Для работы с этим разделом необходимо перейти в режим **Управление системой**. Этот режим доступен только пользователям с ролью «Администратор».

На странице **Журналы** можно задать следующие настройки:

- **Каталог журнала** — каталог, в котором должны храниться файлы журналов.

  > Путь к файлам журналов можно изменить в конфигурационном файле.

- **Тип журналирования**

  Возможны следующие значения:

  - **Базовый**

    Kaspersky CyberTrace Service генерирует файлы журналов, которые хранятся в каталоге журналов.

    Вы можете указать для хранилища журналов следующие ограничения: по размеру одного файла журнала или по размеру всех журналов (в мегабайтах).

    В разделе **Ограничить размер файла** введите желаемый размер файла в поле **Максимальный размер файла (МБ)**.

    В разделе **Ограничить размер всех журналов** введите желаемый размер журналов в поле **Максимальный размер журнала (МБ)**.

    Если не требуется ограничивать размер одного файла журнала или общий размер всех журналов, включите переключатель **Неограниченный**.

По умолчанию переключатель **Неограниченный** включен как для размера одного файла журнала, так и для общего размера всех журналов.

Если переключатель **Неограниченный** включен как для размера одного файла журнала, так и для общего размера всех журналов, поля для ввода ограничений будут неактивны.

Если переключатель **Неограниченный** включен для общего размера всех журналов, можно установить ограничение на размер одного файла журнала.

Если переключатель **Неограниченный** отключен как для размера одного файла журнала, так и для общего размера всех журналов, ограничения можно установить как для размера отдельных файлов журнала, так и для общего размера всех журналов. Размер одного файла журнала не должен превышать общего размера всех журналов.

Ошибка может возникнуть в следующих случаях:

- размер одного файла журнала превышает общий размер всех журналов;
- при выключенном переключателе **Неограниченный** не указаны ограничения на размеры.

- **Syslog**

  За ведение журнала отвечает демон syslog. Это возможно только при установке Kaspersky CyberTrace на устройстве с ОС Linux.

- **Уровень ведения журналов**

  Возможны следующие значения:

  - **Выключено**

    Ведение журналов отключено.

    Соответствует уровню ведения журналов `non` в конфигурационном файле kl_feed_service_log.conf.

  - **Ошибка**

    Регистрируются только ошибки.

    Соответствует уровню ведения журналов `err` в конфигурационном файле kl_feed_service_log.conf.

  - **Информация**

    Регистрируются ошибки и информационные сообщения.

    Соответствует уровню ведения журналов `inf` в конфигурационном файле kl_feed_service_log.conf.

  - **Отладка**

    Регистрируются все сообщения.

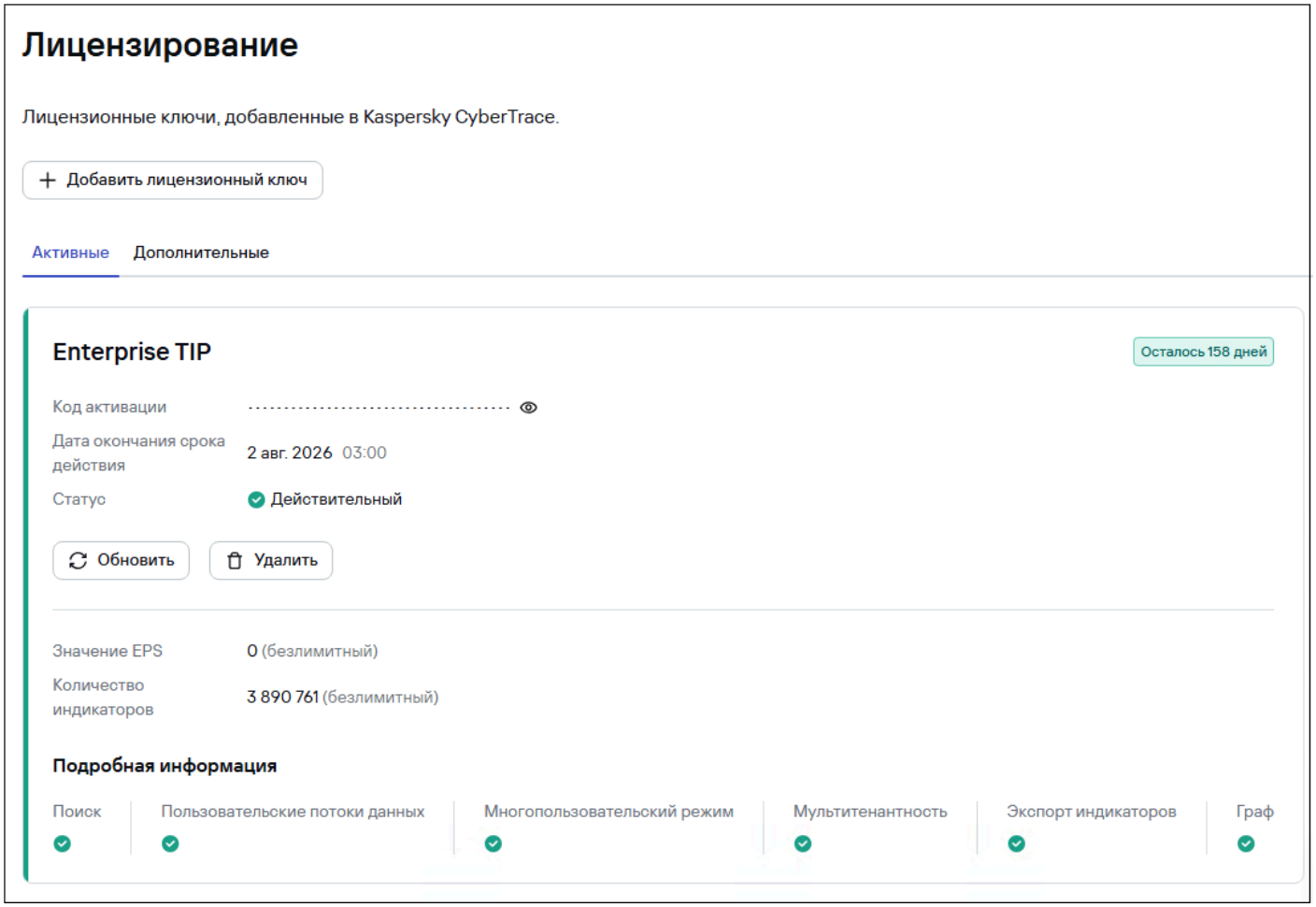
    Соответствует уровню ведения журналов `any` в конфигурационном файле kl_feed_service_log.conf.

- **Удалять старые журналы при запуске Kaspersky CyberTrace** — если этот параметр включен, файлы журналов, созданные в прошлые сеансы, удаляются. Этот параметр доступен, только если задан **Тип журналирования** – **Базовый**.

Подробнее о содержимом файла журнала.

Настройка лицензирования

Управлять лицензированием Kaspersky CyberTrace можно в веб-интерфейсе Kaspersky CyberTrace на странице **Параметры** → **Лицензирование**. Для работы с этим разделом необходимо перейти в режим Управление системой. Этот режим доступен только пользователям с ролью «Администратор».



Страница **Лицензирование**

На странице **Лицензирование** две вкладки: с активными и дополнительными лицензионными ключами.

Для каждого лицензионного ключа предоставляется следующая информация:

- Уровень лицензирования ключа.
- Количество дней до истечения срока действия лицензионного ключа.
- Имя файла лицензионного ключа. Отображается только в том случае, если лицензионный ключ был добавлен с помощью файла ключа.
- Дата и время окончания срока действия ключа. Время указывается в вашем часовом поясе.
- Статус истечения срока действия ключа — *Действительный*, *Срок действия истекает* или *Срок действия истек*.
- Ограничение на количество событий в секунду (EPS).
- Текущее количество индикаторов, загруженных в Kaspersky CyberTrace.

  Этот элемент показывает количество уникальных индикаторов для всех включенных источников данных об угрозах. Также обратите внимание, что если один и тот же индикатор присутствует у нескольких источников данных об угрозах, дубликаты этого индикатора не учитываются при подсчете общего количества.

- Максимальное количество индикаторов, разрешенное на данном уровне лицензирования.
- Информация о доступности функции поиска в веб-интерфейсе Kaspersky CyberTrace.
- Информация о возможности использования пользовательских потоков данных об угрозах.
- Информация о том, позволяет ли лицензия создавать нескольких пользователей.
- Информация о том, позволяет ли лицензия работать с несколькими тенантами.
- Информация о том, позволяет ли лицензия экспортировать индикаторы.
- Информация о том, позволяет ли лицензия использовать графы.
- Информация о том, позволяет ли лицензия использовать обогащение индикаторов из стороннего источника.
- Информация о том, доступен ли раздел **Отчеты**.
- Информация о том, доступен ли аудит действий пользователей.

О лицензировании

В этом разделе приводится описание уровней лицензирования Kaspersky CyberTrace.

Коммерческие уровни лицензирования и Community Edition

Политика лицензирования Kaspersky CyberTrace предусматривает два типа лицензирования:

- Community Edition

  Это ограниченный уровень лицензирования, в котором Kaspersky CyberTrace можно использовать без лицензионного ключа. Community Edition можно использовать для ознакомительных целей. Этот уровень лицензирования не предусматривает срока действия.

  Если лицензионный ключ не добавлен, используется уровень лицензирования Community Edition.

  Уровень лицензирования Community Edition имеет следующие ограничения:

  - Многопользовательский режим недоступен. В Kaspersky CyberTrace имеется единственная учетная запись с ролью «Администратор», которая может выполнять все операции.
  - Обрабатывается не более 250 событий в секунду.

    Если вы приняли Положение о Kaspersky Security Network, максимальное количество событий в секунду увеличивается до 500.
  - Из всех потоков данных об угрозах можно загрузить не более 1 000 000 записей.

- Коммерческое лицензирование

  Эти уровни лицензирования доступны с лицензионным ключом и подходят для различных сценариев использования Kaspersky CyberTrace в организации.

  Чтобы получить лицензионный ключ, обратитесь к своему менеджеру по работе с клиентами.

  Лицензионный ключ можно добавить в Kaspersky CyberTrace посредством кода активации или файла лицензионного ключа. Лицензионные ключи, добавляемые через код активации, имеют ряд отличий от лицензионных ключей, добавляемых через файл ключа.

Различия лицензионных ключей, добавляемых через код активации и через файл ключа

Параметр	Лицензионный ключ, добавляемый с помощью кода активации	Лицензионный ключ, добавляемый с помощью файла ключа
Период между уведомлением о скором истечении срока действия лицензионного ключа и фактическим истечением срока действия	Короче	Длиннее
Порядок замены лицензионного ключа для продолжения использования Kaspersky CyberTrace	Запросите продление лицензионного ключа у своего менеджера по работе с клиентами. Информация в Kaspersky CyberTrace обновляется автоматически или вручную.	Получите новый лицензионный ключ у вашего менеджера по работе с клиентами и затем добавьте лицензионный ключ в Kaspersky CyberTrace.

Приоритеты уровней лицензирования

Ниже приведен список уровней лицензирования, начиная с наивысшего приоритета:

- Enterprise TIP
- Matching Engine
- Community Edition

Информация, содержащаяся в лицензионном ключе

Лицензионный ключ представляет собой последовательность битов, применение которой дает возможность использовать определенный уровень лицензирования Kaspersky CyberTrace.

Лицензионный ключ содержит следующую информацию:

- Уровень лицензирования
- Дата окончания срока действия
- Ограничение на количество событий в секунду (EPS)
- Ограничение на общее количество индикаторов, которые могут быть загружены из потоков данных об угрозах Kaspersky Threat Data Feeds

Кроме того, в лицензионном ключе перечислены доступные функции.

Лицензионные ключи хранятся в каталоге %service_dir%/httpsrv/lic. Для управления лицензионными ключами используется вкладка **Параметры → Лицензирование**.

Если срок действия лицензионного ключа истек или скоро истечет, Kaspersky CyberTrace отображает уведомления и отправляет оповещения о событиях.

Активные и дополнительные лицензионные ключи

Лицензионный ключ может быть активным или дополнительным.

Активный лицензионный ключ — это лицензионный ключ, который Kaspersky CyberTrace использует в текущий момент. В Kaspersky CyberTrace не может быть больше одного активного лицензионного ключа.

Если есть всего один неистекший лицензионный ключ, в качестве активного используется этот ключ. Если есть несколько неистекших лицензионных ключей, выбирается лицензионный ключ со сроком действия, ближайшим к истечению. Если истек срок действия всех ключей, используется уровень лицензирования Community Edition.

Дополнительный лицензионный ключ — это лицензионный ключ, который в настоящее время не используется. Дополнительный лицензионный ключ автоматически становится активным, когда срок действия текущего активного лицензионного ключа истекает. Дополнительный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа.

При добавлении нового лицензионного ключа Kaspersky CyberTrace выбирает активный лицензионный ключ, удовлетворяющий следующим критериям:

- Если активный лицензионный ключ добавлен с помощью кода активации:
  - Добавление второго лицензионного ключа с помощью кода активации не допускается.
  - При добавлении нового лицензионного ключа с помощью файл ключа старый лицензионный ключ, добавленный с помощью кода активации, остается активным.
- Если активный лицензионный ключ добавлен с помощью файла ключа:
  - Когда новый лицензионный ключ добавляется с помощью кода активации, этот новый лицензионный ключ становится активным.
  - Когда новый лицензионный ключ добавляется с помощью файла ключа, активный лицензионный ключ сравнивается с новым лицензионным ключом:
    - Выбирается тот лицензионный ключ, у которого срок действия истекает раньше.
    - Если у обоих лицензионных ключей одинаковая дата истечения срока действия, выбирается лицензионный ключ с более приоритетным уровнем лицензирования.
    - Если у лицензионных ключей одинаковый уровень лицензирования, может быть выбран любой из ключей.

Лицензирование и DMZ

Демилитаризованной зоной (DMZ) называется сегмент локальной сети, в котором находятся серверы, отвечающие на запросы из глобальной сети. Для обеспечения безопасности локальной сети организации доступ к локальной сети из демилитаризованной зоны осуществляется через межсетевой экран.

Kaspersky CyberTrace не отправляет какую-либо информацию о лицензии в «Лабораторию Касперского». Механизмы лицензирования остаются работоспособными в сценариях с DMZ.

Если Kaspersky CyberTrace используется в сценарии с «демилитаризованной зоной» (DMZ), лицензионный ключ можно добавить только с помощью файла лицензионного ключа.

Ограничения, накладываемые лицензионными ключами

В этом разделе описываются ограничения, налагаемые на функциональные возможности Kaspersky CyberTrace лицензионными ключами разных уровней лицензирования.

Ограничение на количество событий в секунду (EPS)

На уровне лицензирования Community Edition количество событий в секунду, обрабатываемых Kaspersky CyberTrace, ограничено параметрами данного уровня лицензирования (по умолчанию 250 событий в секунду). Максимальное количество событий в секунду можно увеличить до 500, приняв Положение о Kaspersky Security Network.

Для ряда уровней коммерческого лицензирования в лицензионном ключе указываются ограничения на количество событий в секунду (EPS). Kaspersky CyberTrace ограничивает EPS для этих уровней лицензирования в два этапа.

На первом этапе, если в какой-либо момент времени ограничение на EPS оказывается превышено, Kaspersky CyberTrace отображает уведомление в веб-интерфейсе Kaspersky CyberTrace и генерирует оповещение `KL_ALERT_EPSLimitExceeded`. Все события свыше ограничения EPS продолжают обрабатываться.

На втором этапе, если семь дней подряд средний EPS системы, рассчитанный за один час, превышает пороговый EPS системы в течение более чем 30% времени, ограничение вступает в силу. Kaspersky CyberTrace отображает уведомление в веб-интерфейсе Kaspersky CyberTrace и генерирует оповещение `KL_ALERT_EPSHardLimit`. С этого момента Kaspersky CyberTrace обрабатывает события только в пределах лимита, установленного лицензионным ключом. После замены лицензионного ключа или перехода к обработке количества событий не более предела, заданного лицензионным ключом, это ограничение перестает действовать.

Ограничение количества индикаторов

> Это ограничение относится только к уровню лицензирования Community Edition.

Уровень лицензирования устанавливает ограничение на общее количество индикаторов; Kaspersky CyberTrace считывает в сумме не больше записей из всех потоков данных, чем разрешено лицензионным ключом или уровнем лицензирования.

Если количество индикаторов превышает лимит, Kaspersky CyberTrace отправляет событие `KL_ALERT_IndicatorsStoreHardLimit`, а затем отображает в веб-интерфейсе Kaspersky CyberTrace уведомление о наличии ограничения на добавление и обновление индикаторов. При генерации события `KL_ALERT_IndicatorsStoreHardLimit` Kaspersky CyberTrace перестает считывать новые записи.

После замены лицензионного ключа или перехода к обработке количества индикаторов не более предела, заданного лицензионным ключом, это ограничение перестает действовать.

Ограничение на использование пользовательских потоков данных об угрозах

Если лицензионный ключ не позволяет использовать пользовательские потоки данных, можно использовать только потоки данных «Лаборатории Касперского» об угрозах. Потоки данных об угрозах OSINT в этом случае использовать нельзя.

Прочие ограничения

Доступность следующих функций зависит от лицензионного ключа или уровня лицензирования:

- Поиск в веб-интерфейсе Kaspersky CyberTrace
- Добавление сторонних потоков данных

- Многопользовательский режим

  Если доступен многопользовательский режим, можно создавать пользователей и управлять ими.

  В противном случае вход возможен только с учетной записью `admin`. Эта учетная запись обладает ролью «Администратор».

- Режим мультитенантности

  Если включен режим мультитенантности, можно создавать тенанты и управлять ими.

  В противном случае можно использовать только тенант по умолчанию.

- Экспорт IoC
- Использование графов
- Рассылка статистических отчетов по электронной почте
- Внешние источники:
  - Обогащение индикаторов из Kaspersky Threat Intelligence Portal
  - Скачивание отчетов из Kaspersky Threat Intelligence Portal
- Аудит действий пользователей:
  - Настройка аудита действий пользователей
  - Скачивание журнала аудита действий пользователей

Добавление лицензионного ключа

Добавить в Kaspersky CyberTrace активный лицензионный ключ или дополнительный лицензионный ключ можно с помощью веб-интерфейса.

Чтобы добавить лицензионный ключ, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите на страницу **Параметры** → **Лицензирование**.
2. Нажмите на кнопку **Добавить лицензионный ключ**.

   Откроется окно **Добавление лицензионного ключа**.
3. Выберите метод добавления лицензионного ключа: с помощью кода активации или с помощью файла лицензионного ключа.

4. В зависимости от выбранного метода выполните следующие действия:

   - Введите код активации, полученный от вашего менеджера по работе с клиентами.

     Код активации состоит из четырех блоков по пять символов.

   - Нажмите кнопку **Выбрать**, затем выберите файл лицензионного ключа, полученный от вашего менеджера по работе с клиентами.

5. Нажмите на кнопку **Добавить**.

   Kaspersky CyberTrace добавляет лицензионный ключ в репозиторий. Если активный лицензионный ключ отсутствует, добавленный ключ становится активным. В противном случае он добавляется в качестве дополнительного лицензионного ключа.

Удаление лицензионного ключа

Удалить лицензионные ключи можно с помощью веб-интерфейса Kaspersky CyberTrace.

Чтобы удалить лицензионный ключ, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите на страницу **Параметры** → **Лицензирование**.

2. Нажмите на кнопку **Удалить** для лицензионного ключа, который требуется удалить.

3. В открывшемся окне подтверждения нажмите кнопку **Удалить** для подтверждения удаления.

   Выбранный лицензионный ключ удаляется из репозитория.

Обновление информации о лицензионном ключе

Обновить информацию можно только о лицензионном ключе, добавленном в Kaspersky CyberTrace с помощью кода активации.

Чтобы продолжить использование Kaspersky CyberTrace после истечения срока действия лицензионного ключа, необходимо запросить продление лицензионного ключа у вашего менеджера по работе с клиентами. После продления лицензионного ключа информация в Kaspersky CyberTrace автоматически обновится не позднее, чем через 24 часа с момента продления. В неотложных случаях информацию о лицензионном ключе можно обновить вручную, как описано в этом разделе.

Порядок обновления информации о лицензионном ключе:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите на страницу **Параметры** → **Лицензирование**.

2. Нажмите на кнопку **Обновить** для требуемого лицензионного ключа.

   Информация о выбранном лицензионном ключе обновляется.

Работа с тенантами

В этом разделе описывается порядок настройки тенанта.

Роль «Администратор» позволяет управлять всеми тенантами, добавленными в Kaspersky CyberTrace. Пользователи с ролью «Менеджер тенанта» могут управлять только теми тенантами, к которым им предоставлен доступ. У пользователей с ролью «Аналитик» нет доступа к этим страницам.

Для работы с веб-страницами, описанными в этом разделе, необходимо перейти в режим **Управление данными**.

Общая настройка тенанта

Управлять общими параметрами определенного тенанта можно в веб-интерфейсе Kaspersky CyberTrace на странице **Параметры** → **Общие**. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Чтобы изменить общие параметры тенанта, выполните следующие действия:

1. Введите имя нового тенанта в поле **Имя тенанта**.

   Длина имени тенанта должна составлять от 1 до 64 символов. Допускаются латинские буквы, цифры, специальные символы (" ', . @ # $ % & * № / \) и пробелы.

   > Изменить имя тенанта «General» невозможно.

2. Введите описание этого тенанта в поле **Описание**.

   Длина описания тенанта должна составлять от 0 до 2048 символов. Допускаются латинские буквы, цифры, специальные символы (" ', . @ # $ % & * № / \), пробелы и переносы строки.

3. В разделе **Пороговый EPS тенанта** настройте пороговый EPS тенанта (число событий в секунду — events per second):

   a. Включите переключатель.

   b. В поле **Пороговый EPS** введите требуемое значение порогового EPS.

   > Если значение EPS приближается к пороговому значению, в веб-интерфейсе отображается предупреждение и генерируется оповещение с предупреждением. При превышении лимита в рамках тенанта сверхлимитный трафик для этого тенанта сбрасывается, отображается предупреждение и генерируется оповещение с предупреждением. Если пороговый EPS тенанта не задан, это может повлиять на другие тенанты (если таковые имеются).

4. В разделе **Входящие события** задайте параметры сокета данного тенанта, который Kaspersky CyberTrace должен прослушивать в ожидании входящих событий:

   a. Выберите тип соединения, который требуется использовать: **IP-адрес и порт** или **Сокет UNIX**.

   b. В зависимости от типа подключения выполните одно из следующих действий:

   - Укажите IP-адрес и порт в полях **IP-адрес** и **Порт**.
   - В поле **Сокет UNIX** укажите сокет UNIX.

   c. Если выбран тип соединения **IP-адрес и порт**, в поле **Защищенное соединение** выберите тип соединения: **TLS** или **Нет**.

5. В блоке **Оповещения об обнаружении индикаторов компрометации** укажите следующие параметры:

   a. В полях **IP-адрес или имя хоста** и **Порт** укажите IP-адрес и порт для конкретного тенанта, которые Kaspersky CyberTrace будет использовать для исходящих оповещений об обнаружении индикаторов компрометации.

   b. В поле **Secure connection** выберите тип соединения: **TLS с проверкой сертификата**, **TLS без проверки сертификата** или **Нет**.

6. В разделе **Служебные оповещения** настройте отправку служебных оповещений, посредством которых другое ПО (например, SIEM-система) снабжается информацией о состоянии тенанта:

   a. Включите переключатель.

   b. В полях **IP-адрес** и **Порт** укажите параметры сервера, на который требуется отправлять служебные оповещения.

   По умолчанию указаны IP-адрес `127.0.0.1` и порт `9999`.

   > Поддерживается отправка служебных оповещений на адреса IPv6.

   c. В поле **Secure connection** выберите тип соединения: **TLS с проверкой сертификата**, **TLS без проверки сертификата** или **Нет**.

7. Включите эту функцию в разделе **Поиск через API**, если требуется сохранять обнаружения киберугроз, связанные с индикаторами, и вести статистику по индикаторам, полученным через общедоступные API с помощью методов поиска.

   По умолчанию эта функция включена.

   > Получение статистики по данным, получаемым через общедоступные API с помощью методов поиска, требует дополнительных вычислительных ресурсов. Чтобы избежать снижения производительности, можно отредактировать раздел `<Source id="api_single_lookup">` конфигурационного файла `kl_feed_service.conf` и изменить регулярные выражения на «(.*)». Это, однако, может привести к неправильному расчету статистики.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Обновленные общие параметры тенанта сохраняются.

Сброс статистики

Это действие убирает с информационной панели всю статистику обнаружений киберугроз, связанную с тенантом. Эту операцию могут выполнять только пользователи с ролью «Администратор».

Рекомендуется выполнить эту операцию после успешной интеграции Kaspersky CyberTrace с SIEM-системой. Это означает, что на информационной панели не будут отображаться оповещения об обнаружении индикаторов компрометации, сгенерированные во время проверки работоспособности, а будут отображаться только реальные оповещения об обнаружении индикаторов компрометации, если таковые имеются.

Чтобы сбросить статистику тенанта, выполните следующие действия:

1. Нажмите на кнопку ↺ (**Сбросить статистику**) на странице **Параметры** → **Общие**.
2. В открывшемся окне подтверждения нажмите кнопку **Сбросить**.

   Статистика тенанта будет сброшена.

Настройка служебных оповещений тенанта

Служебные оповещения представляют собой исходящие сообщения, информирующие целевое программное обеспечение (например SIEM-систему) о статусе тенанта.

Настройка служебных оповещений для тенанта выполняется в веб-интерфейсе Kaspersky CyberTrace на странице **Параметры** → **Служебные оповещения**. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Для тенантов предусмотрены такие же параметры служебных оповещений, как и для службы Kaspersky CyberTrace.

Служебные оповещения, отправляемые для тенанта

В этом разделе приводится описание служебных оповещений для тенантов, которые может генерировать Kaspersky CyberTrace.

KL_ALERT_FeedEnabled

Это оповещение создается при включении потока данных тенанта.

У этого оповещения есть следующее поле:

- *feed*

  Имя потока данных об угрозах.

KL_ALERT_FeedDisabled

Это оповещение создается при отключении потока данных тенанта.

У этого оповещения есть следующее поле:

- *feed*

  Имя потока данных об угрозах.

KL_ALERT_ServiceUnavailable

Это оповещение генерируется, когда модуль мониторинга работоспособности обнаруживает сбой или зависание Kaspersky CyberTrace Service.

У этого оповещения нет полей контекста.

KL_ALERT_ServiceStopped

Это оповещение генерируется при успешной остановке Kaspersky CyberTrace Service.

У этого оповещения нет полей контекста.

KL_ALERT_ServiceStarted

Это оповещение генерируется при успешном запуске Kaspersky CyberTrace Service.

У этого оповещения нет полей контекста.

KL_ALERT_EPSHardLimit

Это предупреждение создается, если текущий EPS тенанта превышает пороговый EPS тенанта.

Оповещение отправляется не чаще одного раза в час.

У этого оповещения есть следующие поля:

- *tenant_limit_eps*

  Пороговый EPS тенанта.

- *current_tenant_eps*

  Текущий EPS тенанта на момент превышения лимита.

Настройка потоков данных тенанта

Управлять параметрами потоков данных тенанта можно в веб-интерфейсе Kaspersky CyberTrace на странице **Параметры → Потоки данных**.

Для работы с этой страницей необходимо перейти в режим **Управление данными**.

В отличие от режима **Управление системой**, в режиме **Управление данными** для потока данных можно задать лишь некоторые параметры, перечисленные ниже.

> Управлять можно только теми потоками данных, которые включены в режиме **Управление системой**.

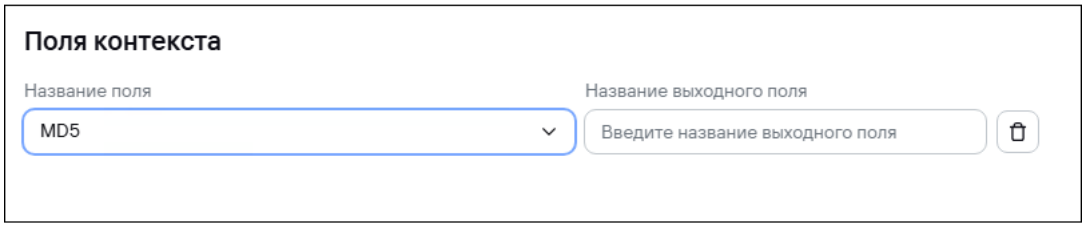
Для определенного тенанта форма позволяет выполнять следующие действия:

- Включение и отключение потоков данных об угрозах
- Выбор доступных полей для потока данных об угрозах
- Добавление в поток данных полей контекста (см. описание ниже)

Добавление полей контекста в поток данных

В этом разделе описывается порядок добавления дополнительных полей к исходящим оповещениям, которые отправляет Kaspersky CyberTrace.

Поля контекста — это поля, которые можно вставлять в исходящие оповещения отдельно от контекста записей потока данных об угрозах. Поля контекста можно использовать для извлечения конкретной информации из контекста и передачи ее в отдельные поля.



Работа с полями контекста

Чтобы добавить поля контекста для потока данных об угрозах, выполните следующие действия:

1. Перейдите на страницу **Параметры → Потоки данных**.
2. В столбце **Действия** списка потоков данных выберите поток данных, который требуется настроить.
3. В разделе настроек потока данных об угрозах найдите раздел **Поля контекста**.

4. В поле ввода **Название поля** укажите имя одного из полей в исходном потоке данных об угрозах.

   Если запись потока данных об угрозах содержит несколько полей с одинаковыми именами и это имя упоминается в списке полей контекста, в исходящее оповещение будут включены значения всех этих полей, перечисленные в одном поле через точку с запятой.

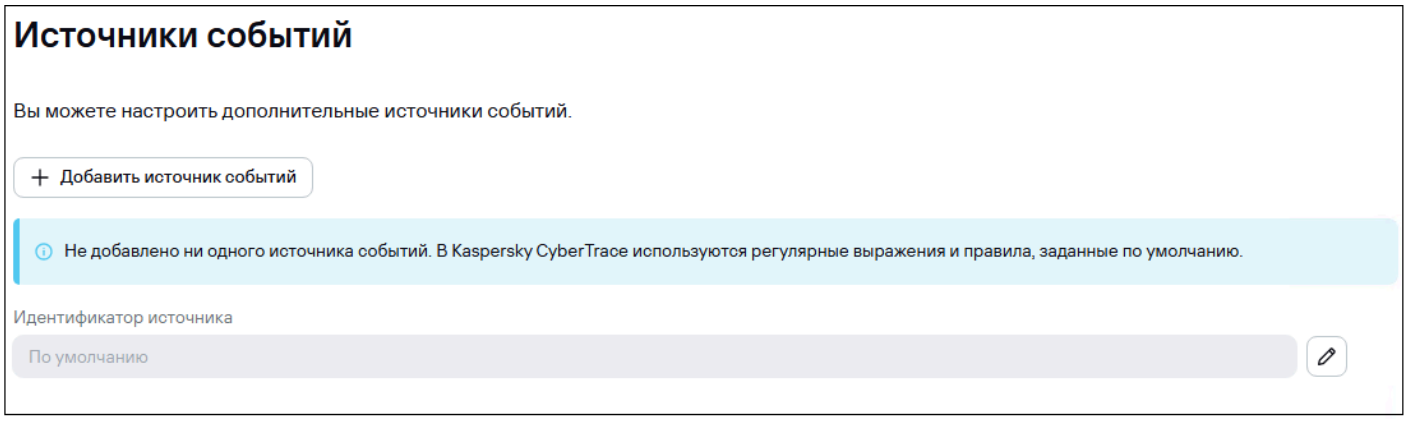
5. В поле ввода **Название выходного поля** укажите имя поля в том виде, как оно будет вставляться в исходящие события.

   Если текстовое поле **Название выходного поля** не заполнено, имя поля в исходящем оповещении будет таким же, как имя поля, указанное в потоке данных об угрозах.

6. Прокрутите страницу до конца и нажмите кнопку **Сохранить**.

Настройка источников событий тенанта

Для настройки источников событий используется страница **Параметры** → **Источники событий**. Для работы с этой страницей необходимо перейти в режим **Управление данными**.



Страница **Параметры** → **Источники событий**

В Kaspersky CyberTrace регулярные выражения и правила нормализации событий сгруппированы по источникам событий. Регулярные выражения и правила нормализации событий, не относящиеся к какому-либо определенному источнику событий, группируются под источником событий `default`. Все регулярные выражения из источника событий `default` копируются в новый источник событий. Для каждого источника событий должно быть задано хотя бы одно регулярное выражение. Источники событий (кроме `default`) можно добавлять и удалять, а также изменять их свойства. Источники событий также можно удалять, кроме источника событий `default`.

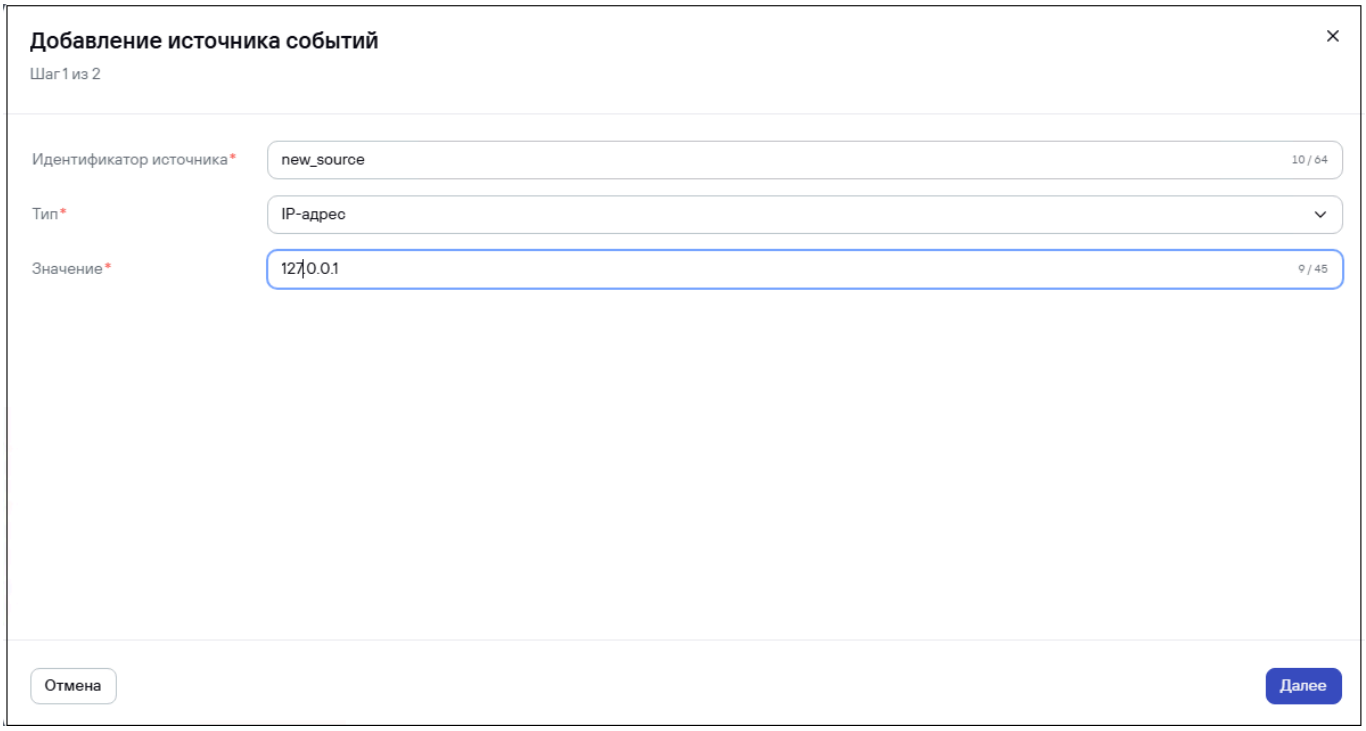
На странице **Источники событий** отображаются все источники событий, определенные в конфигурационном файле Kaspersky CyberTrace Service.

Добавление источника событий

Чтобы добавить источник событий, выберите следующие действия:

1. Нажмите на кнопку **Добавить источник событий**.

Запустится мастер Добавление источника событий.



Мастер Добавление источника событий. Шаг 1

2. Задайте следующие параметры нового источника событий:

   - **Идентификатор источника**

     Имя источника событий. Должно быть уникальным среди используемых имен источников событий. В имени разрешены следующие символы: латинские буквы, цифры, дефис (-), точка (.) и знак подчеркивания (_).

   - **Тип**

     Можно выбрать один из следующих вариантов:

     - **IP-адрес**

       IP-адрес устройства, выдающего события, для которого необходимо добавить правила парсинга.

       Поддерживаются адреса IPv4 и IPv6.

     - **Имя хоста**

       Имя хоста устройства, выдающего события.

       Значение должно совпадать со значением в поле `HOSTNAME` входящих событий syslog от этого источника событий.

     - **Регулярное выражение**

       Регулярное выражение, с которым будет сопоставляться источник в событиях, получаемых Kaspersky CyberTrace. Это регулярное выражение должно быть оптимизированным.

3. Нажмите на кнопку **Далее**.

   Если данные, введенные на предыдущем шаге, верны, откроется форма для задания регулярных выражений и правил нормализации событий (см. подраздел «Форма изменения свойств источника событий» ниже).

Все регулярные выражения из источника событий `default` копируются в новый источник событий. Kaspersky CyberTrace попытается получить данные из полученных событий с использованием скопированных регулярных выражений. Рекомендуется продолжать поиск событий в течение некоторого времени, необходимого для отображения данных в окне мастера.



Мастер Добавление источника событий. Шаг 2.

4. На основе оценки данных в окне мастера задайте регулярные выражения и правила нормализации событий, затем нажмите кнопку **Добавить**.

   Для правил нормализации включите переключатель **Применять правила нормализации**. В противном случае правила нормализации не будут связаны с новым источником событий.

Если введенные свойства источника событий корректны, создается новый источник событий.

Изменение источника событий

Чтобы изменить источник событий, выполните одно из следующих действий:

- Основные параметры источника событий (имя, тип и значение) можно изменить на странице **Источники событий**.

  > Основные параметры источника событий **По умолчанию** изменить невозможно.

- Чтобы изменить правила нормализации событий и регулярные выражения, заданные для источника событий, нажмите кнопку (**Изменить**) рядом с соответствующим источником событий. Открывается форма изменения свойств источника событий (см. подраздел «Форма изменения свойств источника событий» ниже).

Форма изменения свойств источника событий

Форма изменения свойств источника событий (правил нормализации событий и регулярных выражений) разделена на верхнюю и нижнюю области. В верхней области отображаются события и выделяются подстроки, извлеченные с использованием выбранного регулярного выражения. В нижней области две вкладки: **Правила нормализации** и **Регулярные выражения**

При открытии формы изменения свойств источника событий начинается анализ событий, выдаваемых источником событий. Эти события обрабатываются в соответствии с правилами нормализации, а результат отображается в верхней части формы.

> Если указано имя хоста источника событий, но из входящих событий не извлекается поле `HOSTNAME`, события не отображаются. Чтобы решить эту проблему, укажите IP-адрес или регулярное выражение источника событий или измените формат событий.

Анализ поступающих событий в реальном времени можно приостановить, возобновить или перезапустить. При перезапуске анализа входящих событий текстовое поле, в котором отображаются события, очищается. Это текстовое поле может содержать до 100 строк. По мере поступления новых данных старые данные удаляются.

Настройка правил нормализации событий

В нижней области формы изменения свойств источника событий выберите вкладку **Правила нормализации**, чтобы добавить, удалить или изменить правила нормализации, которые будут применяться к входящим событиям, удовлетворяющим условиям источника событий. Можно указать, какие последовательности символов должны заменяться другими (правила замены) и какие последовательности символов должны использоваться для идентификации событий, которые следует игнорировать (правил игнорирования). При выключенном переключателе **Применять правила нормализации** все элементы интерфейса для задания правил нормализации отключаются, и правила нормализации для настраиваемого источника событий не сохраняются.

> В правилах замены не следует указывать символ новой строки (`\n`). Для разделения составных входящих событий на отдельные события используется элемент `InputSettings > EventDelimiter` конфигурационного файла Kaspersky CyberTrace Service.

Для создаваемого источника событий форма на вкладке **Правила нормализации** изначально заполняется правилами нормализации, заданными для источника событий `default`.

Настройка регулярных выражений

В нижней части формы изменения свойств источника событий выберите вкладку **Регулярные выражения**, чтобы добавить, удалить или изменить регулярные выражения, которые будут применяться к входящим событиям, удовлетворяющим условиям источника событий. Для создаваемого источника событий изначально форма на вкладке **Регулярные выражения** заполняется регулярными выражениями, заданными для источника событий `default`, которые извлекают по крайней мере некоторые данные из отображаемых событий.

У регулярных выражений есть следующие свойства:

- Тип индикатора

  Тип данных, извлекаемых из события. Можно выбрать один из следующих типов индикатора:

  - URL
  - MD5
  - SHA1
  - SHA256
  - HASH
  - IP
  - DOMAIN
  - CONTEXT

- Имя регулярного выражения

  Имена регулярных выражений, относящиеся к одному и тому же источнику событий, не должны повторяться.

- Само регулярное выражение

  Регулярное выражение, используемое для извлечения требуемого значения из события.

- Флажок **Извлечь все**

  Если этот флажок снят, регулярное выражение извлекает только первое успешно сопоставленное значение. Если этот флажок установлен, регулярное выражение извлекает все успешно сопоставленные значения.

- Правила конкатенации

  Можно задать способ объединения частей извлеченных данных в единое значение. (Подробнее о составных значениях)



Настройка регулярных выражений и их свойств

Можно выделить значения, соответствующие регулярным выражениям, указанным для источника событий. Щелкните внутри текстового поля, содержащего регулярное выражение, которое требуется выделить.

Удаление источника событий

Чтобы удалить источник событий, выберите следующие действия:

1. Нажмите на кнопку (**Удалить**) рядом с источником событий, который требуется удалить.
2. В открывшемся окне подтверждения нажмите кнопку **Удалить**.

Удаленный источник событий исключается из списка источников событий.

Настройка правил нормализации

В этом разделе описывается порядок настройки правил нормализации источника событий.

О правилах нормализации

Правила нормализации используются для трансформации событий. После того как Kaspersky CyberTrace применит правила нормализации к входящему событию, это событие обрабатывается с помощью регулярных выражений.

Существуют два типа правил нормализации:

- **Правила замены**

  Правила замены одной последовательности символов на другую.

- **Правила игнорирования**

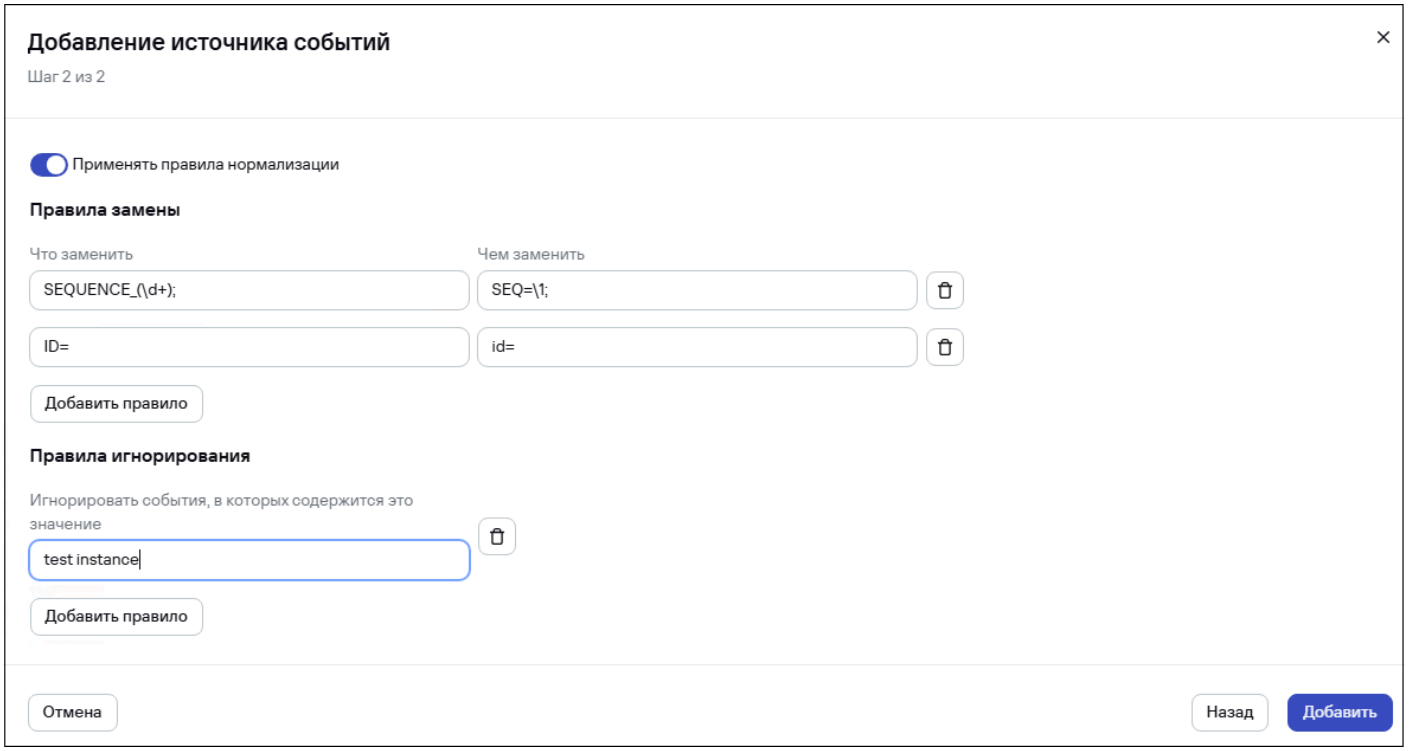
  Правила игнорирования событий, содержащих определенную последовательность символов.

Если заданы и правила замены, и правила игнорирования, сначала применяются правила замены, а затем — правила игнорирования.

В указанных регулярных выражениях звездочка (`*`) и вопросительный знак (`?`) не рассматриваются как подстановочные знаки.

Чтобы настроить правила нормализации, выполните следующие действия:

Начните создавать или изменять источник событий.



Настройка правил нормализации

Добавление правила нормализации

Чтобы добавить правило нормализации, выполните следующие действия:

1. Перейдите на вкладку **Правила нормализации**.
2. Включите переключатель **Применять правила нормализации**.
3. Выполните одно из следующих действий:
   - Чтобы добавить правило замены, выполните следующие действия:
     a. Нажмите на кнопку **Добавить правило** в блоке **Правила замены**.
     b. Укажите регулярное выражение в поле ввода **Что заменить** и замену в поле ввода **Чем заменить**.
   - Чтобы добавить правило игнорирования, выполните следующие действия:
     a. Нажмите на кнопку **Добавить правило** в блоке **Правила игнорирования**.
     b. Укажите регулярное выражение в поле **Игнорировать события, в которых содержится это значение**.
4. Нажмите на кнопку **Сохранить**.

Новое правило нормализации добавляется в список правил нормализации.

Изменение правила нормализации

Чтобы изменить правило нормализации, выполните следующие действия:

1. Перейдите на вкладку **Правила нормализации**.
2. Найдите необходимое правило нормализации.
3. Внесите требуемые изменения в полях ввода.
4. Нажмите на кнопку **Сохранить**.

Правило нормализации отображается в списке правил нормализации с внесенными изменениями.

Удаление правила нормализации

Чтобы удалить правило нормализации, выполните следующие действия:

1. Перейдите на вкладку **Правила нормализации**.
2. Нажмите на кнопку (**Удалить**) рядом с правилом нормализации, которое требуется удалить.
3. Нажмите на кнопку **Сохранить**.

Удаленное правило нормализации исключается из списка правил нормализации.

О регулярных выражениях

В этом разделе описываются регулярные выражения и приводятся сведения об их использовании.

О регулярных выражениях

Регулярные выражения используются для анализа входящих событий, обрабатываемых правилами нормализации. Регулярные выражения извлекают информацию, которая должна быть проверена в потоках данных об угрозах и использована в исходящих оповещениях.

Предустановленные регулярные выражения соответствуют формату событий, используемых в самостоятельной диагностике.

После выполнения проверки работоспособности может потребоваться добавить ряд новых регулярных выражений или изменить существующие регулярные выражения для использования с конкретным программным обеспечением, выступающим в качестве источника событий. Примеры регулярных выражений для анализа событий, выдаваемых популярными устройствами, приведены в разделе Регулярные выражения для популярных устройств.

Рекомендуется задать регулярные выражения для извлечения данных, таких как IP-адрес и порт источника событий, а также цели события, имени пользователя и даты. Эти регулярные выражения задают формат исходящих оповещений.

Об именах регулярных выражений

Для регулярного выражения можно использовать любые имена кроме следующих:

- `SourceId`
- `MatchedIndicator`
- `RecordContext`
- `Category`
- `ActionableFields`
- `Confidence`
- `IndicatorInfo`
- `EventReceivedDate`
- `Ретроскан`

Составные значения

Атрибут `concatenate` используется для определения правила, используемого для формирования составного значения из данных, извлеченных из события. Правило оперирует группами извлеченных данных посредством символов `#N`, где N — номер группы (начиная с 1). Если перед символом решетки (`#`) стоит обратная косая черта (\), то символ решетки рассматривается не как часть номера группы, а как собственно символ решетки.

Рассмотрим парсинг на примере следующего события:

```
url_1=http://domain test_event url_2=/page/mypage test
```

Используемые регулярные выражения и соответствующие результаты парсинга примера события представлены в таблице ниже.

Примеры применения регулярных выражений

Регулярное выражение	Результат парсинга
`<RE_URL concatenate="#1#2">url_1=(.*?)\stest_event\surl_2=(.*?)\stest</RE_URL>`	http://domain/page/mypage
`<RE_URL concatenate="#2#1">url_1=(.*?)\stest_event\surl_2=(.*?)\stest</RE_URL>`	/page/mypagehttp://domain
`<RE_URL concatenate="#2_/_#1">url_1=(.*?)\stest_event\surl_2=(.*?)\stest</RE_URL>`	/page/mypage_/_http://domain

Если правило конкатенации не задано или атрибут `concatenate` имеет пустое значение, а в регулярном выражении более одной группы, конкатенация значений групп выполняется в том порядке, в котором они входят в регулярное выражении.

Если в атрибуте `concatenate` больше групп, чем в регулярном выражении, дополнительные группы будут игнорируются и заменяются соответствующим текстом `#N`.

Событие, подвергаемое парсингу:

```
url_1=http://domain test_event url_2=/page/my_page test
```

Используемое регулярное выражение:

```
<RE_URL concatenate="#1#2#3">url_1=(.*?)\stest_event\surl_2=(.*?)\stest</RE_URL>
```

Результат парсинга:

```
http://domain/page/my_page#3
```

Несколько совпадений

При парсинге события с помощью регулярного выражения можно извлечь все значения, совпавшие с регулярным выражением. Для этого установите для атрибута `extract` значение `"all"`. Если установлено значение `"first"` или атрибут не указан, извлекается только первое значение, совпавшее с регулярным выражением.

Для каждого совпавшего значения создается отдельное событие обнаружения киберугрозы. Если процесс обнаружения киберугрозы не затрагивает определенное поле события, в качестве значения такого поля в выходном событии используется знак дефиса (-).

Событие для парсинга:

```
ip1=12.12.12.12 ip2=23.23.23.23 hash1=abc hash2=cde    user1=N1    user2=N2
```

Элементы конфигурационного файла:

```
<RegExps>
  <Source id="default">
    <RE_IP extract="all">...</RE_IP>
    <RE_HASH extract="all">...</RE_HASH>
    <RE_USER extract="first">...</RE_USER>
  </Source>
</RegExps>
<EventFormat>ip=%RE_IP%   hash=%RE_HASH%  user=%RE_USER%  %FeedContext%</EventFormat>
```

Доступные записи потока данных:

```
IP = 12.12.12.12
IP = 23.23.23.23
hash = cde
```

Генерируемые события обнаружения киберугроз:

```
ip=12.12.12.12  hash=-    user= N1  <context for 12.12.12.12>
ip=23.23.23.23  hash=-    user= N1  <context for 23.23.23.23>
ip=- hash=cde  user=N1   <context for cde>
```

Указание символов по их шестнадцатеричному коду

Kaspersky CyberTrace Service использует регулярные выражения, соответствующие синтаксису PCRE. Этот синтаксис позволяет указывать символ по его коду несколькими способами.

Kaspersky CyberTrace Service не поддерживает указание символов в формате `\x{hhh..}`. Вместо этого укажите символ по его коду следующим образом: `\uhhhh`, где `hhhh` – шестнадцатеричный код символа. Например, вместо выражения `([\x{00a1}-\x{ffff}])` можно использовать выражение `([\u00a1-\uffff])`.

Оптимизация регулярных выражений

Оптимизация регулярных выражений позволяет предотвратить поиск с возвратом, который затрудняет сопоставление строки.

Для оптимизации регулярных выражений придерживайтесь следующих правил:

- Используйте сверхжадные квантификаторы `(++, *+)`.
- Если возможно, используйте группу без сопоставления `(?:)` с внешними скобками.
- Старайтесь как можно реже использовать оператор альтернативы и находить совпадения в конце строки. Оператор альтернативы имеет самый низкий приоритет среди всех операторов регулярных выражений.
- Используйте символы начала и конца строки `(^, $)`.
- Используйте атомарные группы. Атомарные группы автоматически отбрасывают все позиции возврата, запомненные любыми токенами внутри данной группы. Используется синтаксис `(?> ...)`.
- В длинных регулярных выражениях старайтесь избегать экспоненциального роста возвратов. Не рекомендуется использовать конструкции вроде `(qwerty.*)*`

Настройка источников событий с помощью пользовательских регулярных выражений

В данном разделе описывается порядок добавления и настройки источников событий с пользовательскими регулярными выражениями.

Kaspersky CyberTrace отправляет оповещение об обнаружении киберугрозы в SIEM-систему в виде единого события. В это событие должна быть включена вся контекстная информация, необходимая для оценки и расследования киберугрозы, включая специфическую информацию для конкретных исходных источников событий. Этого можно добиться путем настройки источников событий и пользовательских регулярных выражений.

Повторите описанные ниже шаги для каждого имеющегося уникального источника событий.

Чтобы настроить источник событий с пользовательскими регулярными выражениями, выполните следующие действия:

1. Создайте источник событий.
2. В дополнение к регулярным выражениям для индикаторов (`URL`, `IP`, `MD5` и другие типы индикаторов) добавьте регулярные выражения типа `CONTEXT`. Регулярные выражения типа `CONTEXT` могут сопоставляться с любой полезной информацией, такой как идентификаторы событий, идентификаторы запросов, метки времени и др. Данная контекстная информация помогает при поиске необработанных событий в SIEM.
3. Рекомендуется заменить универсальные регулярные выражения для индикаторов регулярными выражениями, соответствующими формату события, который использует данный источник событий. Регулярные выражения для многих популярных устройств описаны в разделе Регулярные выражения для популярных устройств.
4. Добавьте все регулярные выражения типа `CONTEXT` в поле **Формат оповещения**. Для этого укажите имена всех регулярных выражений в формате оповещений об обнаружении индикаторов компрометации с использованием шаблона `%RegexpName%`.

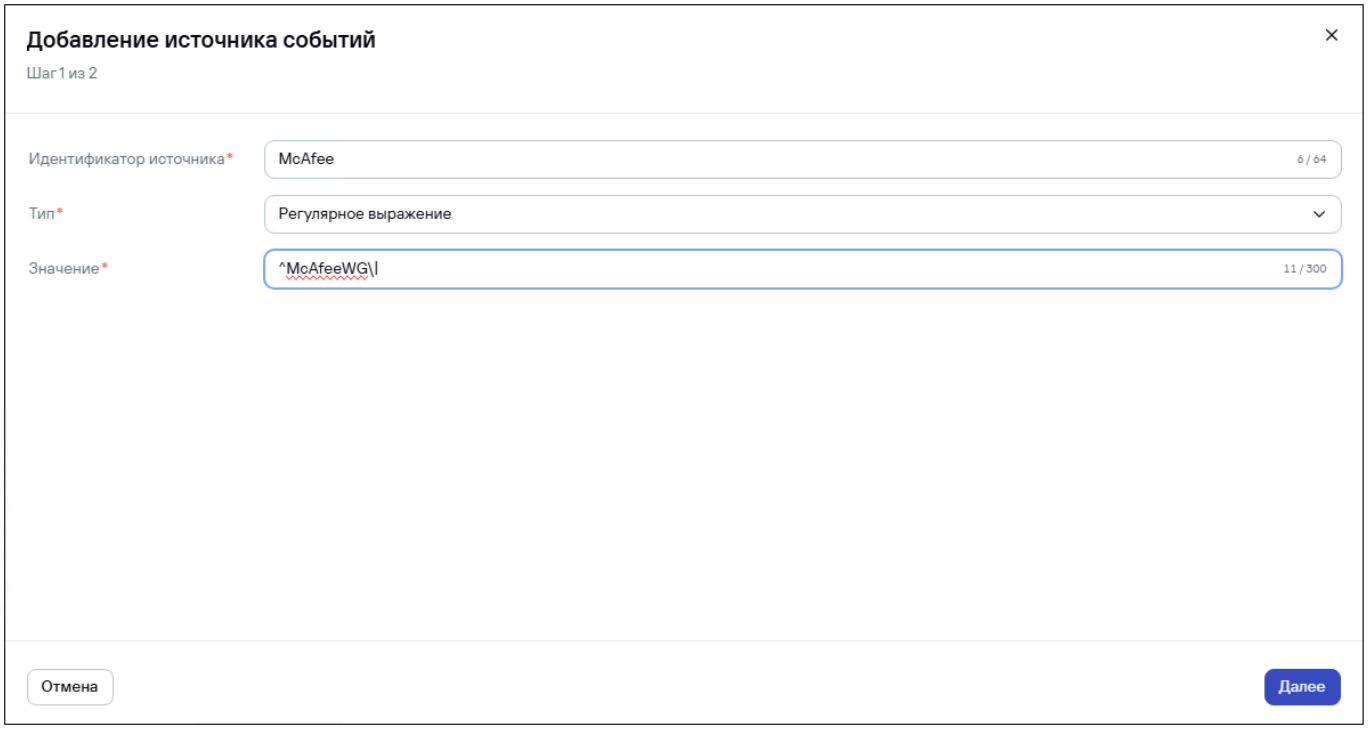
Пример

Источником событий в этом примере является источник McAfee Web Gateway.

Чтобы настроить источник событий с пользовательскими регулярными выражениями, выполните следующие действия:

1. Создайте источник событий.

   Данный источник отправляет журналы событий из SIEM-системы, поэтому добавить этот источник событий по IP-адресу невозможно, поскольку у всех таких источников событий будет IP-адрес SIEM-системы. Вместо этого укажите регулярное выражение, которое будет идентифицировать данный источник событий на основе данных, содержащихся в событиях. Например, выражение может сопоставлять имя устройства или версию устройства, которые указываются в событиях. Обратите внимание: если источник событий отправляет события напрямую в Kaspersky CyberTrace, такой источник может быть идентифицирован по его IP-адресу.



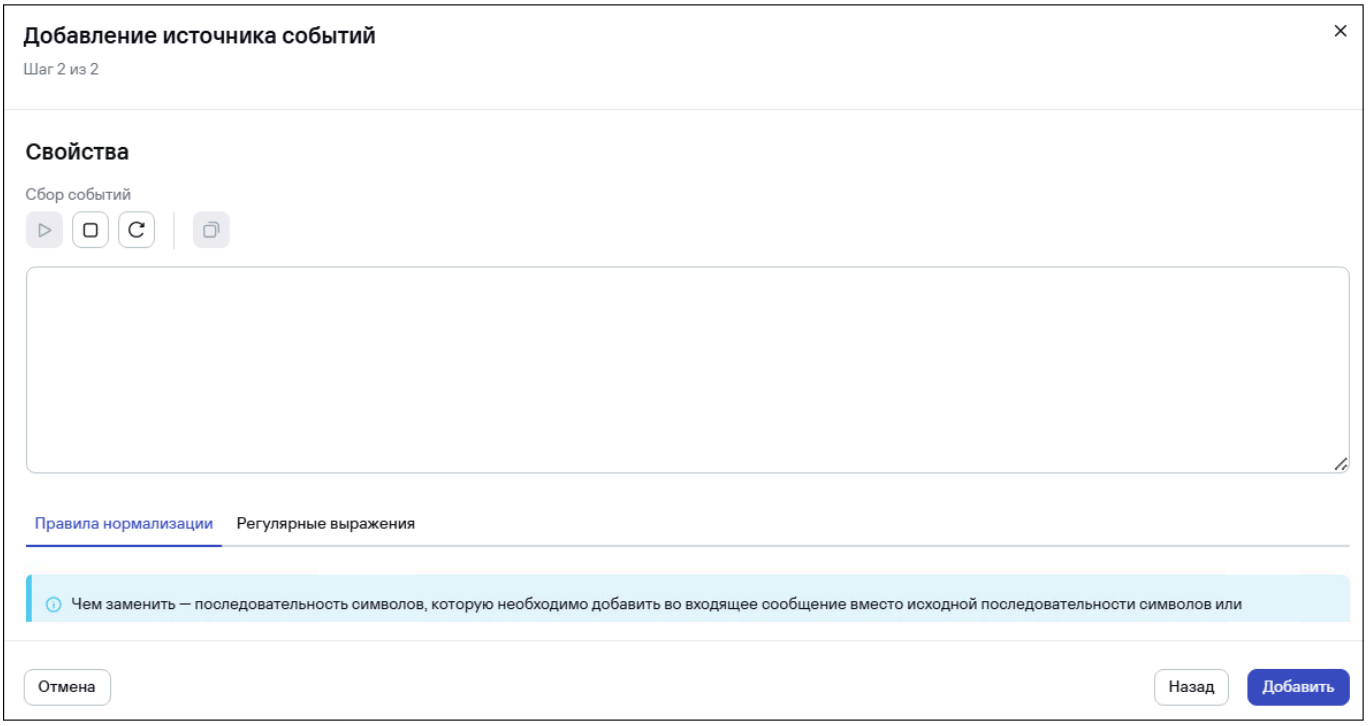
Создание источника событий

2. Начните анализ событий и получите несколько событий.

   Отображаются только те события, которые сопоставляются с регулярным выражением, указанным на предыдущем шаге.

   Допустим, что были получены события со следующими данными:

```
McAfeeWG|time_stamp=[01/Jan/2015:02:12:31
+0800]|auth_user=jsmith|src_ip=10.10.69.1|server_ip=192.0.2.1|host=www.example.com|url_
Software/Hardware|rep_level=Minimal
Risk|method=GET|url=http://www.example.com/|media_type=text/html|application_name=|user
(compatible; MSIE 10.0; Windows NT 6.2; WOW64;
Trident/6.0)|block_res=0|block_reason=|virus_name=|hash=|filename=|filesize=753|
```



Анализ событий

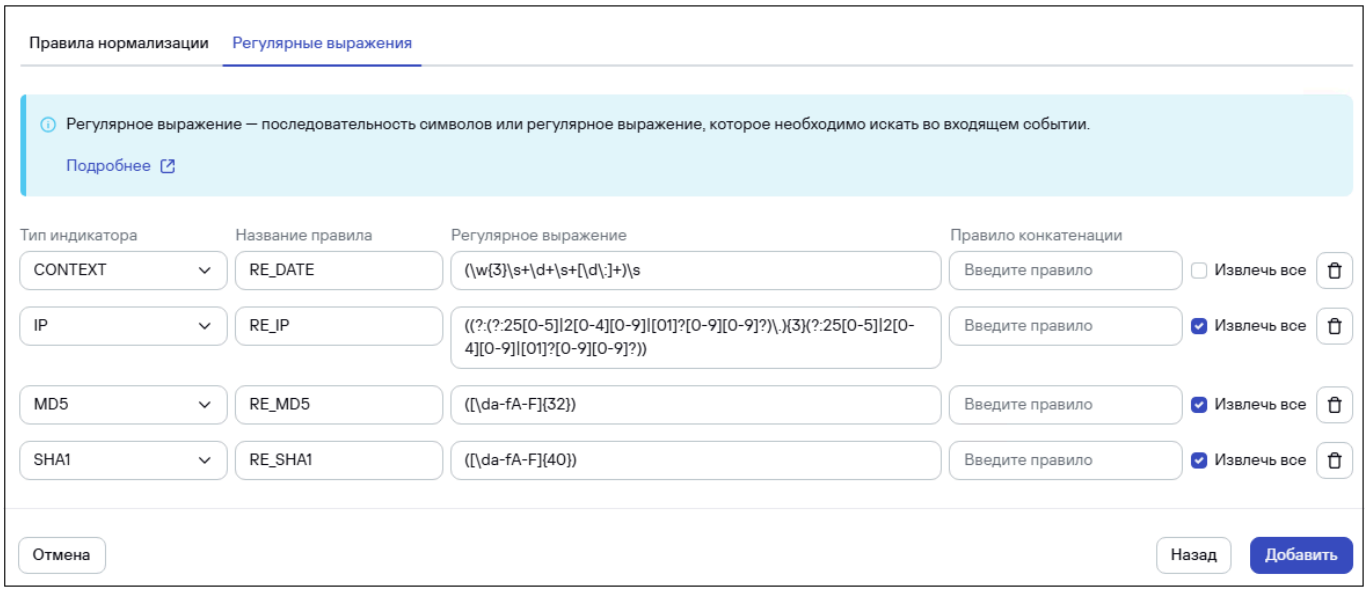
3. Остановите анализ событий. Регулярные выражения для URL и IP-адресов будут заданы автоматически. При необходимости замените эти универсальные выражения специальными. Затем добавьте регулярные выражения типа `CONTEXT`.

   Для сопоставления имени пользователя, содержащегося в событиях, добавьте выражение с именем `RE_USERNAME`. Укажите следующее значение для выражения: `auth_user\=(.*?)(?:\|)`

   Для сопоставления исходного IP-адреса добавьте выражение с именем `RE_SRCIP`. Укажите следующее значение для выражения: `src_ip\=(.*?)(?:\|)`

   Для сопоставления URL добавьте выражение с именем `RE_URL`. Укажите следующее значение для выражения: `url\=(.*?)(?:\|)`

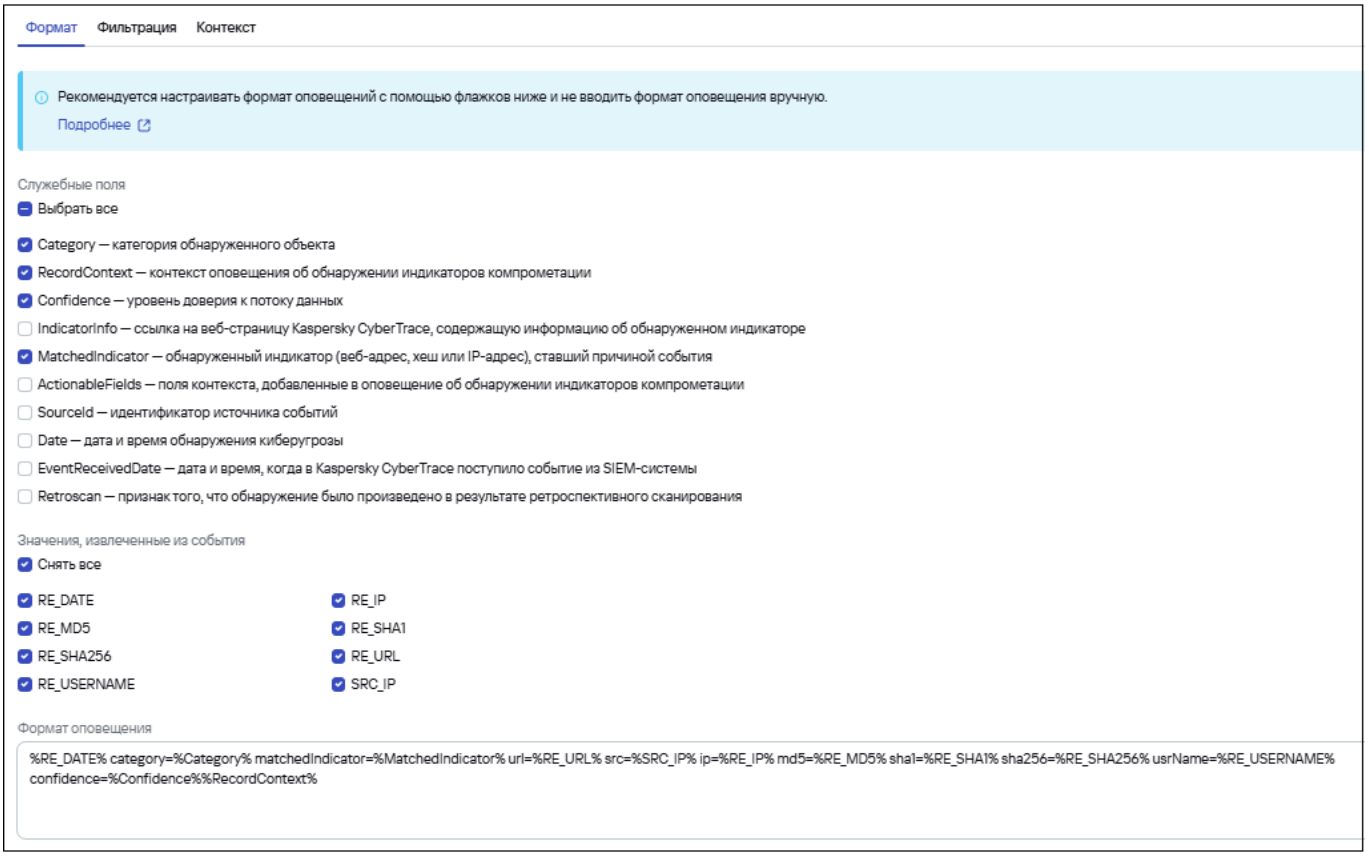
Для сопоставления кода статуса HTTP добавьте выражение `RE_HTTPCODE`. Укажите следующее значение для выражения: `status_code=(\d+)`



Указание пользовательских регулярных выражений

4. Задайте формат оповещений об обнаружении индикаторов компрометации, содержащий эти регулярные выражения:

   ```
   eventName=%Category% matchedIndicator=%MatchedIndicator% url=%RE_URL% src=%RE_SRCIP%
   ip=%RE_IP% http_code=%RE_HTTPCODE% usrName=%RE_USERNAME% %RecordContext%
   ```



Задание формата вывода оповещений об обнаружении индикаторов компрометации

После выполнения описанных выше действий оповещения об обнаружении индикаторов компрометации будут содержать поля контекста. Например, оповещение из Kaspersky CyberTrace может содержать следующую информацию:

```
device=McAfee eventName=KL_IP_Reputation matchedIndicator=192.0.2.1 url=- src=10.10.69.1
ip=192.0.2.1 http_code=301 category=test usrName=jsmith first_seen=01.01.2017 00:00
ip=192.0.2.1 ip_geo=ru last_seen=20.11.2019 10:02 popularity=1 threat_score=75
```

Регулярные выражения для популярных источников событий

В этом разделе представлены регулярные выражения, предназначенные для использования при анализе событий, выдаваемых популярными источниками событий.

> У разных версий определенных источников событий формат генерируемых событий может отличаться, поэтому регулярные выражения, приведенные в данном разделе, могут оказаться неактуальными. В этом случае следует скорректировать предлагаемые регулярные выражения.

Устройства FireEye

События, поступающие от продуктов FireEye, требуют следующих регулярных выражений:

- События в формате CEF

Поле	Регулярное выражение
URL1	`filePath=([^\s]*?)\s`
URL2	`cs5=([^\s]*?)\s`
MD5	`fileHash=([^\s]*?)\s`
SrcIp	`src=([^\s]*?)\s`
DstIp	`dst=([^\s]*?)\s`

- События в формате CEF

Поле	Регулярное выражение
URL1	`cnchost=([^,]*?),`
URL2	`objurl=([^,]*?),`
MD5	`fileHash=([^,]*?),`
SrcIp	`src=([^,]*?),`
DstIp	`dst=([^,]*?),`

Устройства Blue Coat SG

События, поступающие от продуктов Blue Coat® SG, требуют следующих регулярных выражений:

- События SYSLOG

Поле	Регулярное выражение
URL	`OBSERVED\s"(?:.*?)"\s(.*?)\s`
URL2	`http\s(.*?)\s\d+\s(.*?)\s`

Устройства Websense

События, поступающие от продуктов Websense, требуют следующих регулярных выражений:

- События CEF

Поле	Регулярное выражение
URL	`request\=(.*?)(?:\s|$)`
IP Address	`dst\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})(?:\s|$)`

- События LEEF

Поле	Регулярное выражение
URL	`url\=(.*?)(?:\s|$)`
IP Address	`dst\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})(?:\s|$)`

- пары ключ-значение

Поле	Регулярное выражение
URL	`url\=(.*?)(?:\s|$)`
IP Address	`dst_ip\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})(?:\s|$)`

Squid

События, поступающие от продукта Squid, требуют следующих регулярных выражений:

Поле	Регулярное выражение
URL	`(?:GET|POST)\s(.*?)(?:\s)`

Устройства McAfee Web Gateway

События, поступающие от продуктов McAfee® Web Gateway, требуют следующих регулярных выражений:

- Стандартные события

Поле	Регулярное выражение
URL	`url\=(.*?)(?:|)`
IP Address	`server_ip\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})(?:|)`

- События CEF

Поле	Регулярное выражение
URL	`request\=(.*?)(?:\s|$)`
IP Address	`dst\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})(?:\s|$)`

- События SYSLOG

Поле	Регулярное выражение
URL	`(?:GET|POST)\s(.*?)(?:\s)`

Устройства Check Point URL Filtering

Для событий от продуктов Check Point URL Filtering требуются следующие регулярные выражения:

- События SYSLOG

Поле	Регулярное выражение
IP Address	`(?:dst)\s(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})`

Устройства Juniper Networks SRX

События, поступающие от продуктов Juniper Networks SRX, требуют следующих регулярных выражений:

- События SYSLOG

Поле	Регулярное выражение
IP Address	`(?:\sdestination-address)\="(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"\s`

Устройства Check Point Firewall

События, поступающие от продуктов Check Point Firewall, требуют следующих регулярных выражений:

- События SYSLOG

Поле	Регулярное выражение
IP Address	`dst\:(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})`

Palo Alto Networks

События, поступающие от продуктов Palo Alto Networks, требуют следующих регулярных выражений:

- События LEEF

Поле	Регулярное выражение
IP Address	`dst\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})(?:\s|$)`

- События SYSLOG

Поле	Регулярное выражение
IP Address	`(?:dst.*?)(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})`

- События CEF

Поле	Регулярное выражение
IP Address	`dst\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})(?:\s|$)`

Устройства Fortinet FortiGate

События, поступающие от продуктов Fortinet FortiGate, требуют следующих регулярных выражений:

- События SYSLOG

Поле	Регулярное выражение
IP Address	`(?:dst.*?)(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})`

Устройства Cisco IPS

События, поступающие от продуктов Cisco IPS, требуют следующих регулярных выражений:

Поле	Регулярное выражение
IP Address	`(?:dst.*?|to.*?|Dst.*?)(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})`

Устройства Snort

События, поступающие от продукта Snort®, требуют следующих регулярных выражений:

- События UNIFIED2

Поле	Регулярное выражение
IP Address	`(?:destination.*?)(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})`

- CSV-события

Поле	Регулярное выражение
IP Address	`(?:.*?,.*?,.*?,.*?,)(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})`

В качестве альтернативы можно использовать следующие регулярные выражения для парсинга событий всех типов:

Поле	Регулярное выражение
IP Address	`(?:destination.*?|.*?,.*?,.*?,.*?,)(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})`

Устройства Cisco IronPort

События, поступающие от продуктов Cisco IronPort®, требуют следующих регулярных выражений:

- События SYSLOG

Поле	Регулярное выражение
URL	`(?:GET|POST)\s(.*?)\s`
IP Address	`(?:NONE|DIRECT|DEFAULT_PARENT)\/(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})`

Настройка оповещений об обнаружении индикаторов компрометации для тенанта

Для управления параметрами оповещений об обнаружении индикаторов компрометации для каждого тенанта в отдельности используется страница **Параметры → Оповещения об обнаружении индикаторов компрометации**.

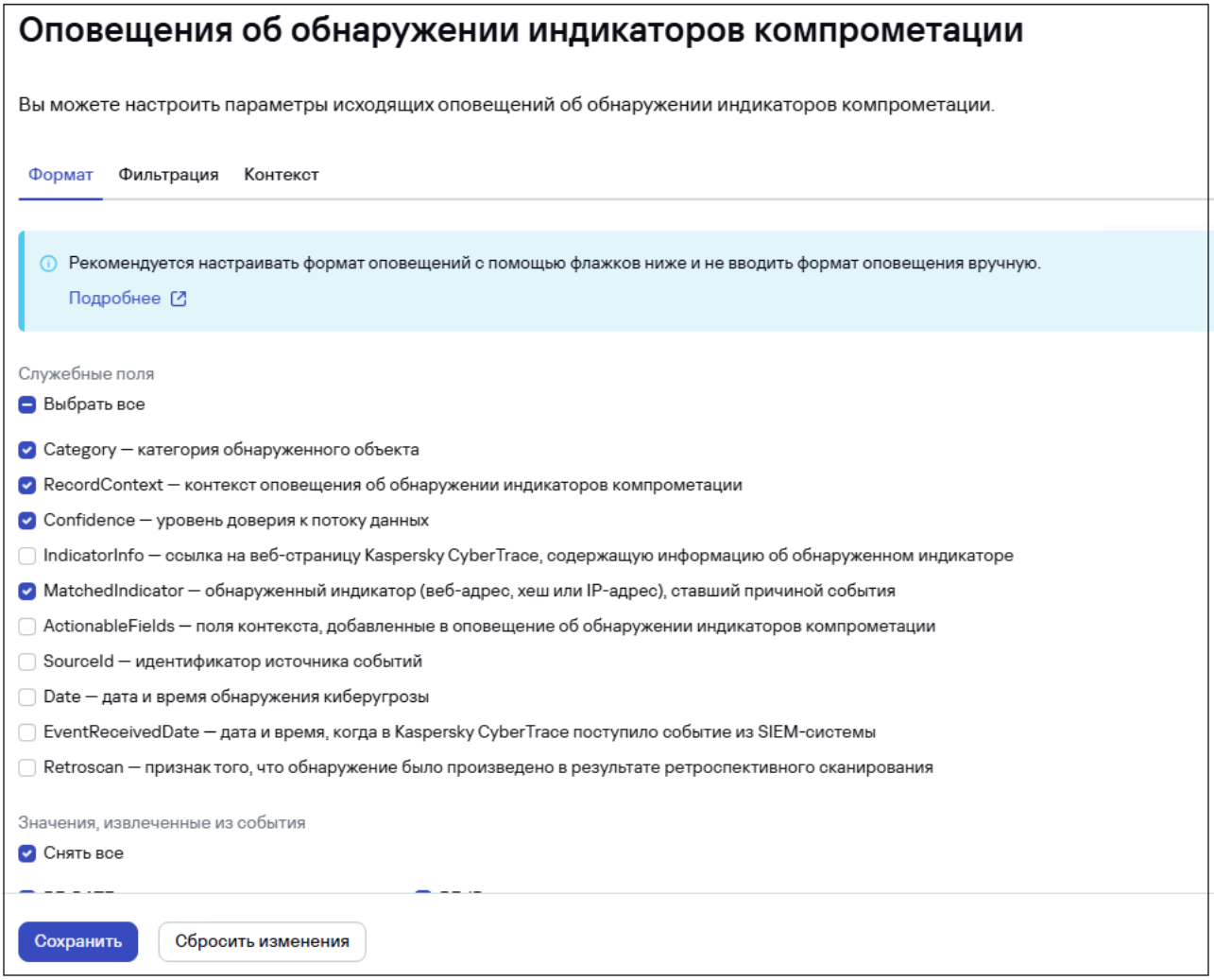
Страница **Оповещения об обнаружении индикаторов компрометации** содержит следующие вкладки:

- **Формат**
- **Фильтрация**
- **Контекст**

Настройка формата оповещений об обнаружении индикаторов компрометации

Оповещения об обнаружении индикаторов компрометации, содержащие информацию об обнаруженных совпадениях с индикаторами.

Вкладка **Формат** страницы **Параметры** → **Оповещения об обнаружении индикаторов компрометации** позволяет задавать формат исходящих оповещений об обнаружении индикаторов компрометации.



Вкладка **Формат** страницы **Параметры** → **Оповещения об обнаружении индикаторов компрометации**

Изменять формат оповещений вручную не рекомендуется. Вместо этого установите флажки для шаблонов, которые требуется использовать в оповещениях, после чего Kaspersky CyberTrace автоматически обновит формат.

Эта вкладка состоит из двух разделов:

- **Служебные поля**

  Значения этих полей представляют собой шаблоны, сгенерированные Kaspersky CyberTrace.

  Установите флажки для шаблонов, которые требуется использовать в исходящих оповещениях об обнаружении индикаторов компрометации. Kaspersky CyberTrace автоматически обновит формат в поле **Формат оповещения**.

- **Значения, извлеченные из события**

Значения этих полей извлекаются из входящих событий с помощью регулярных выражений, определенных для данного источника событий.

Установите флажки для шаблонов, которые требуется использовать в исходящих оповещениях об обнаружении индикаторов компрометации. Kaspersky CyberTrace автоматически обновит формат в поле **Формат оповещения**.

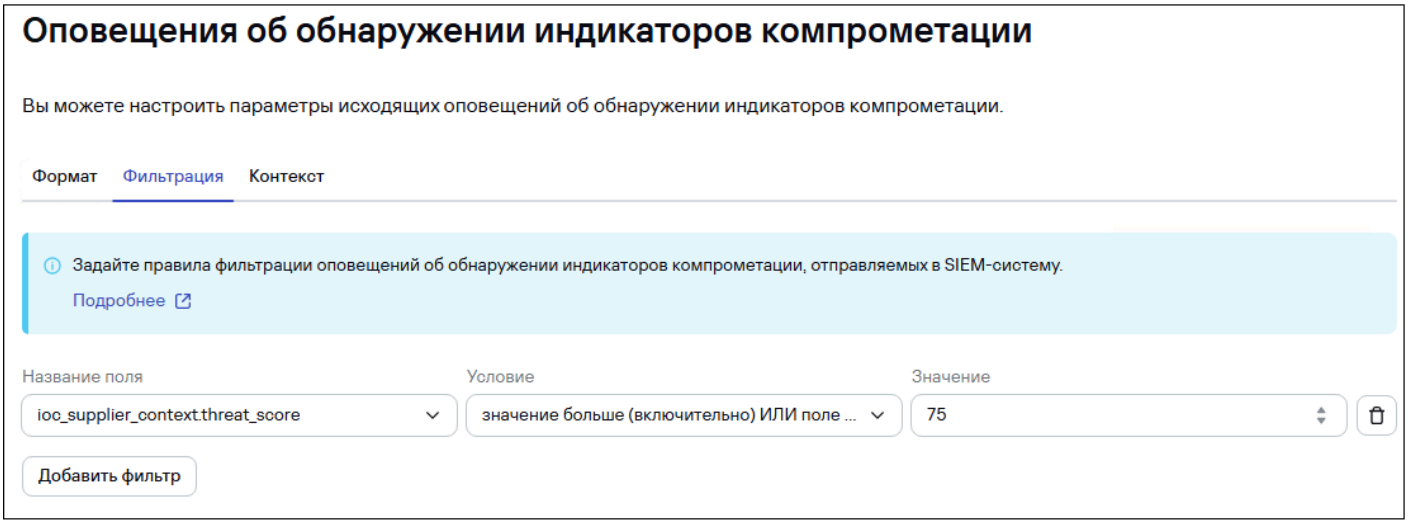
Настройка форматов событий и оповещений для определенных SIEM-систем

Правильный формат оповещений о событиях и оповещениях об обнаружении индикаторов компрометации зависит от используемой SIEM-системы. В случае изменения формата событий или оповещений в Kaspersky CyberTrace также может потребоваться перенастройка интеграции с SIEM-системой.

- В случае ArcSight, возможно, потребуется обновить форматы событий и поля контекста.
- В случае QRadar, возможно, потребуется добавить парсинг новых полей.
- В случае RSA NetWitness, возможно, потребуется указать способ парсинга новых полей (см. также раздел Устранение неполадок RSA NetWitness).
- В случае LogRhythm, возможно, потребуется задать способ парсинга новых полей.

Настройка правил фильтрации для оповещений об обнаружении индикаторов компрометации

На вкладке **Фильтрация** страницы **Параметры → Оповещения об обнаружении индикаторов компрометации** можно задать правила фильтрации оповещений об обнаружении индикаторов компрометации, отправляемых из Kaspersky CyberTrace в SIEM-систему



Вкладка **Фильтрация** страницы **Параметры → Оповещения об обнаружении индикаторов компрометации**

Kaspersky CyberTrace будет отправлять оповещения об обнаружении индикаторов компрометации только в том случае, если для флага отправки оповещений в SIEM-систему (атрибут события `ioc_supplier_send_match` из базы данных индикаторов) установлено значение `true`, а все поля записи потока данных, соответствующие индикатору, удовлетворяют критериям фильтрации. Обратите внимание, что если у обнаруженного индикатора нет атрибута, указанного в правиле фильтрации, считается, что этот индикатор удовлетворяет условиям фильтрации. Однако все оповещения об обнаружении индикаторов компрометации включаются в статистику и отображаются на страницах **Информационная панель** и **Обнаружения**.

Чтобы настроить фильтры для оповещений об обнаружении индикаторов компрометации, выполните следующие действия:

1. В раскрывающемся списке **Название поля** выберите значение, соответствующее имени атрибута индикатора из базы данных индикаторов, к которой применяются правила фильтрации. В раскрывающемся списке **Условие** выберите условие фильтрации.

2. В поле ввода **Значение** укажите значение фильтрации.

   Значения в этом поле запрещается разделять точкой с запятой («`;`»). Вместо этого выберите **значение среди перечисленных (разделенные новой строкой) ИЛИ поле отсутствует** в раскрывающемся списке **Условие** и используйте символ переноса строк («`\n`») или нажимайте клавишу **`Enter`**. В противном случае фильтр не будет применяться правильным образом.

3. Если требуется добавить новый фильтр оповещений, нажмите на кнопку **Добавить фильтр**.

При необходимости любые правила фильтрации можно изменить или удалить.

О критериях фильтрации оповещений, отправляемых в SIEM-систему

В Kaspersky CyberTrace можно задавать правила фильтрации оповещений об обнаружении индикаторов компрометации. Имя атрибута индикатора задается из базы данных индикаторов, а условия фильтрации и значения фильтрации задаются в раскрывающемся списке **Название поля**, в раскрывающемся списке **Условие** и в поле ввода **Значение** соответственно. Обратите внимание, что если у обнаруженного индикатора нет атрибута, указанного в правиле фильтрации, считается, что этот индикатор удовлетворяет условиям фильтрации.

Kaspersky CyberTrace будет отправлять оповещения об обнаружении индикаторов компрометации только в том случае, если для флага отправки оповещений в SIEM-систему (атрибут `ioc_supplier_send_match_event` из базы данных индикаторов) установлено значение `true`, а все поля записи потока данных, соответствующие индикатору, удовлетворяют критериям фильтрации.

Если отключить сохранение оповещений об обнаружении индикаторов компрометации при применении критериев фильтрации для отправки оповещений в SIEM, то оповещения, содержащие индикаторы, не соответствующие указанным критериям, будут отбрасываться.

В таблице ниже перечислены условия фильтрации, которые можно применить к оповещениям об обнаружении индикаторов компрометации:

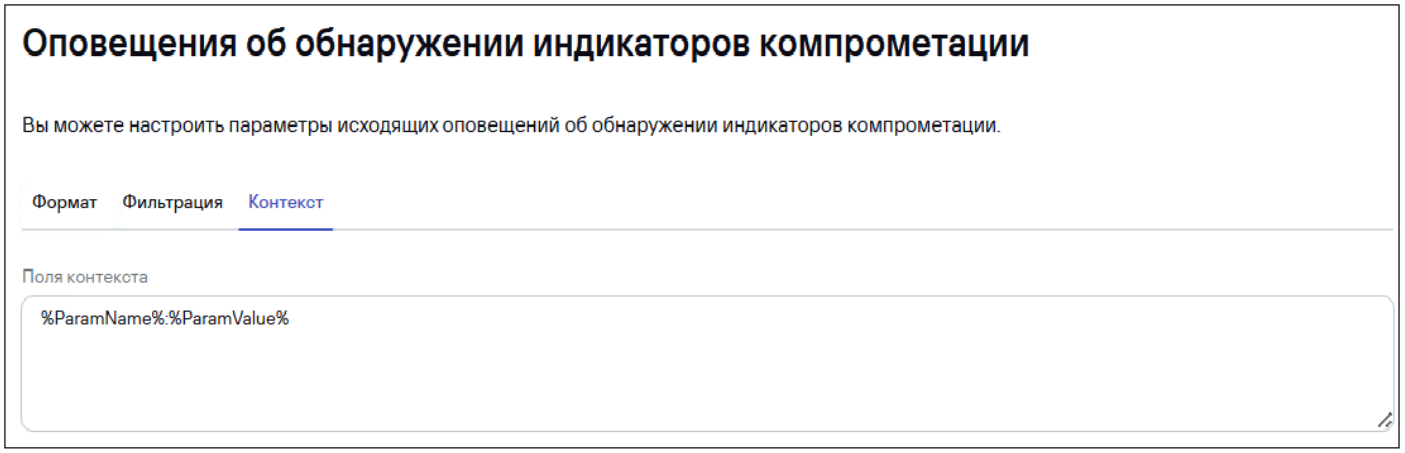
Возможные условия фильтрации

Условие фильтрации	Описание
Равно определенному значению	Атрибут индикатора равен указанному значению. Чтобы применить это условие, выберите **значение равно ИЛИ поле отсутствует** в раскрывающемся списке **Условие**, затем укажите одно значение в поле ввода **Значение**.
Равно хотя бы одному из нескольких значений	Атрибут индикатора должен содержать одно или несколько указанных значений. Чтобы применить это условие, выберите **значение среди перечисленных (разделенные новой строкой) ИЛИ поле отсутствует** в раскрывающемся списке **Условие**, затем укажите несколько значений в поле ввода **Значение**. Не указывайте пустые значения. Каждое следующее значение должно начинаться с новой строки.

Принадлежит к диапазону числовых значений	Атрибут индикатора должен содержать значение в указанном диапазоне. Чтобы применить это условие, выберите **значение в диапазоне (включительно) ИЛИ поле отсутствует** в раскрывающемся списке **Условие**, затем укажите диапазон значений в полях ввода **Значение**. Обратите внимание, что граничные значения включаются в диапазон. Значения должны быть целыми числами.
Принадлежит к диапазону числовых значений, которые больше или равны указанному значению	Атрибут индикатора должен содержать значение, которое больше или равно указанному значению. Чтобы применить это условие, выберите **значение больше (включительно) ИЛИ поле отсутствует** в раскрывающемся списке **Условие**, затем укажите одно значение в поле ввода **Значение**. Значение должно быть целым числом.
Принадлежит к диапазону числовых значений, которые меньше или равны указанному значению	Атрибут индикатора должен содержать значение, которое меньше или равно указанному значению. Чтобы применить это условие, выберите **значение меньше (включительно) ИЛИ поле отсутствует** в раскрывающемся списке **Условие**, затем укажите одно значение в поле ввода **Значение**. Значение должно быть целым числом.
Принадлежит к диапазону дат	Атрибут индикатора должен содержать дату в указанном диапазоне. Чтобы применить это условие, выберите **дата в диапазоне (включительно) ИЛИ поле отсутствует** в раскрывающемся списке **Условие**, затем укажите диапазон дат в полях ввода **Значение**. Чтобы выбрать диапазон дат, используйте средство выбора дат в календаре. Кроме того, при указании границ диапазона можно выбрать произвольное количество дней или одно из следующих предустановленных значений: • **День** • **Неделя** • **Месяц** • **3 месяца**
Принадлежит к диапазону дат, которые больше или равны указанному значению	Атрибут индикатора должен содержать дату, равную указанному значению или превышающую его. Чтобы применить это условие, выберите **дата больше (включительно) ИЛИ поле отсутствует** в раскрывающемся списке **Условие**, затем укажите дату в поле ввода **Значение**. Чтобы выбрать дату, используйте средство выбора дат в календаре. Кроме того, для границы можно выбрать одно из следующих предустановленных значений: • **1 day ago** • **7 days ago** • **30 days ago**
Принадлежит к диапазону дат, которые меньше или равны указанному значению	Атрибут индикатора должен содержать дату, которая меньше или равна указанному значению. Чтобы применить это условие, выберите **дата меньше (включительно) ИЛИ поле отсутствует** в раскрывающемся списке **Условие**, затем укажите дату в поле ввода **Значение**. Чтобы выбрать дату, используйте средство выбора дат в календаре. Кроме того, для границы можно выбрать одно из следующих предустановленных значений: • **1 day ago** • **7 days ago** • **30 days ago**
Равно непустому значению	Атрибут индикатора должен содержать любое непустое значение. Чтобы применить это условие, выберите **значение непустое** в раскрывающемся списке **Условие**.

Настройка контекста оповещений об обнаружении индикаторов компрометации

На вкладке **Контекст** страницы **Параметры → Оповещения об обнаружении индикаторов компрометации** можно задать формат, в котором имена и значения полей контекста потока данных должны вставляться в оповещения об обнаружении индикаторов компрометации, отправляемые из Kaspersky CyberTrace в SIEM-систему.



Вкладка **Контекст** страницы **Параметры → Оповещения об обнаружении индикаторов компрометации**

Чтобы настроить контекст оповещений об обнаружении индикаторов компрометации:

Введите требуемое значение в поле ввода **Поля контекста**.

О шаблонах формата служебных оповещений

Форматы и шаблоны позволяют включать определенную информацию в оповещения об обнаружении индикаторов компрометации, генерируемые Kaspersky CyberTrace.

Форматы — это строки, определяющие формат оповещения или шаблона. *Шаблоны* — это специальные подстановочные строки, которые можно использовать при определении форматов. При генерации оповещения шаблон заменяется фактическими данными.

Формат контекста записи

Формат *%RecordContext%* определяет, каким образом к оповещению должны добавляться поля контекста. Формат этого шаблона можно задать в настройках служебных оповещений.

В формате *%RecordContext%* можно использовать следующие шаблоны:

- *%ParamName%*

  Имя поля в потоке данных.

- *%ParamValue%*

  Значение поля.

Формат *%RecordContext%* определяет формат полей контекста, передаваемых в сообщении об обнаружении киберугрозы.

Например, если для *%RecordContext%* задано `%ParamName%=%ParamValue%`, то для потока данных об угрозах с полями `Ip` и `Geo` может быть получена следующая строка (обратите внимание на пробел между данными двух полей): `"Ip=192.0.2.100 Geo=ru,br,ua,cz,us"`.

Формат полей контекста

Формат *%ActionableFields%* определяет, каким образом к оповещению должны добавляться поля контекста. Для этого шаблона можно задать отдельный формат в настройках контекста оповещений об обнаружении индикаторов компрометации.

В формате *%ActionableFields%* можно использовать следующие шаблоны:

- *%ParamName%*

  Имя поля контекста.

- *%ParamValue%*

  Значение поля контекста.

Формат *%ActionableFields%* определяет формат полей контекста, передаваемых в оповещениях об обнаружении индикаторов компрометации.

Например, если для *%ActionableFields%* задано `%ParamName%:%ParamValue%`, а в потоке данных об угрозах присутствуют поля `cn1` и `cn2`, то может быть получена следующая строка: «`cn1:Example Device cn2:Example Environment`».

Формат оповещений об обнаружении индикаторов компрометации

Этот формат можно указать в настройках формата оповещений об обнаружении индикаторов компрометации.

В этом формате можно использовать следующие шаблоны:

- *%Category%*

  Категория обнаруженного объекта.

- *%RecordContext%*

  Контекст оповещения (см. описание выше в разделе «Формат контекста записи»).

- *%Confidence%*

  Уровень доверия. Это значение берется из значения доверия к индикатору потока данных, содержащего сопоставленные индикаторы из оповещения об обнаружении индикаторов компрометации.

- *%IndicatorInfo%*

  Ссылка на веб-страницу Kaspersky CyberTrace, содержащую информацию об обнаруженном индикаторе.

- *%MatchedIndicator%*

  Обнаруженный индикатор (URL, хеш или IP-адрес), ставший причиной оповещения.

- *%ActionableFields%*

  Поля контекста (см. описание выше в разделе «Формат полей контекста»).

- *%SourceId%*

Идентификатор источника событий. Это имя, указанное для источника событий.

Идентификатор предустановленного источника событий — `Default`.

- *%Date%*

  Текущие дата и время в формате `Mon DD HH:MM:SS`.

- *%EventReceivedDate%*

  Дата и время, когда приложением Kaspersky CyberTrace было получено событие обнаружения из SIEM-системы.

- *%Retroscan%*

  Признак того, что обнаружение было произведено в результате ретроспективного сканирования.

- *Имя регулярного выражения*

  Этот шаблон представляет собой имя регулярного выражения. Шаблон заменяется значением, извлеченным из поля события, сопоставленного с регулярным выражением. Например, если имя регулярного выражения — имя `RE_URL`, шаблон для него — `%RE_URL%`, а сгенерированное оповещение содержит значение, сопоставленное с этим регулярным выражением.

Ниже приведен пример элемента `OutputSettings` > `EventFormat`:

```
%Date% event_name=%Category% source=%SourceId% matchedIndicator=%MatchedIndicator% url=%RE_URL% ip=%RE_IP%
md5=%RE_MD5% sha1=%RE_SHA1% sha256=%RE_SHA256% usrName=%RE_USERNAME% indicatorInfo=%IndicatorInfo%
confidence=%Confidence%%RecordContext%
```

По приведенному выше формату будет сгенерировано следующее оповещение:

```
Apr 16 09:05:41 eventName=KL_Malicious_Hash_MD5 source=ExampleSource
matchedIndicator=C912705B4BBB14EC7E78FA8B370532C9 url=- src=192.0.2.4 ip=192.0.2.23
md5=C912705B4BBB14EC7E78FA8B370532C9 sha1=- sha256=- usrName=ExampleUser
indicatorInfo=https://127.0.0.1/indicators?value=C912705B4BBB14EC7E78FA8B370532C9 confidence=100
MD5=C912705B4BBB14EC7E78FA8B370532C9 SHA1=8CBB395D31A711D683B1E36842AE851D5D000BAD
SHA256=F6E62E9B3AF38A6BF331922B624844AAEB2D3658C4F0A54FA4651EAA6441C933 file_size=2989 first_seen=10.07.2016 23:53
last_seen=13.04.2020 08:08 popularity=1 threat=HEUR:Trojan.Win32.Generic
```

Шаблоны для ArcSight

Для оповещений об обнаружении индикаторов компрометации следует использовать следующий формат:

```
CEF:0|Kaspersky Lab|Kaspersky CyberTrace for ArcSight|2.0|2|CyberTrace Detection Event|8| reason=%Category%
dst=%DST_IP% src=%DeviceIp% fileHash=%RE_HASH% request=%RE_URL% sourceServiceName=%Device% sproc=%Product%
suser=%UserName% msg=CyberTrace detected %Category% externalId=%Id% %ActionableFields% cs5Label=MatchedIndicator
cs5=%MatchedIndicator% cs6Label=Context cs6=%RecordContext%
```

В дополнение к общим шаблонам в формате оповещений об обнаружении индикаторов компрометации для ArcSight используются следующие шаблоны с названиями регулярных выражений:

- `%DST_IP%` — IP-адрес точки назначения.
- `%DeviceIp%` — IP-адрес конечного устройства, на котором произошло событие.
- `%RE_HASH%` — хеш, содержащийся в событии.
- `%RE_URL%` — URL, содержащийся в событии.
- `%Device%` — поставщик устройства.

- `%Product%` — название устройства.
- `%UserName%` — имя пользователя, который был активен на конечном устройстве.
- `%Id%` — идентификатор события.

Шаблоны для RSA NetWitness

> Значения форматов оповещений об обнаружении киберугроз должны соответствовать форматам, заданным в файле v20_cybertracemsg.xml. В случае изменения форматов эти изменения необходимо также перенести в файл v20_cybertracemsg.xml.

Ниже приведен пример формата оповещения об обнаружении индикаторов компрометации:

```
<232>%CyberTrace:MATCH_EVENT
category=%Category%,detected=%MatchedIndicator%,url=%RE_URL%,hash=%RE_HASH%,dst=%DST_IP%,src=%SRC_IP%,dvc=%DeviceIp%,
```

В дополнение к общим шаблонам в формате оповещений об обнаружении индикаторов компрометации для RSA NetWitness используются следующие шаблоны с названиями регулярных выражений:

- `%RE_URL%` — URL, содержащийся в событии.
- `%RE_HASH%` — хеш, содержащийся в событии.
- `%DST_IP%` — IP-адрес точки назначения.
- `%SRC_IP%` — IP-адрес источника.
- `%DeviceIp%` — IP-адрес конечного устройства, на котором произошло событие.
- `%Device%` — поставщик устройства.
- `%DeviceAction%` — действие, выполненное устройством.
- `%UserName%` — имя пользователя, который был активен на конечном устройстве.

Настройка отчетов для тенанта

Kaspersky CyberTrace предоставляет возможность рассылки статистических отчетов по электронной почте. В этом разделе объясняется порядок управления задачами для формирования и рассылки отчетов по электронной почте, а также настройка и составление расписания почтовых рассылок.

Настраивать отчеты тенанта можно в веб-интерфейсе Kaspersky CyberTrace на странице **Параметры** → **Отчеты**. Для работы с этой страницей необходимо перейти в режим **Управление данными**.

Параметры отчетов для тенанта совпадают с параметрами отчетов в режиме **Управление системой**, кроме параметров почтового клиента.

Руководство по Kaspersky CyberTrace Service

В этом разделе описывается принцип действия и порядок настройки Kaspersky CyberTrace Service, а также управление из командной строки или с помощью скриптов.

О Kaspersky CyberTrace Service

Kaspersky CyberTrace Service представляет собой один из компонентов Kaspersky CyberTrace. Он запускается как служба и работает следующим образом:

1. Kaspersky CyberTrace Service прослушивает заданный порт в ожидании входящих событий.
2. Kaspersky CyberTrace Service сопоставляет индикаторы в полученных событиях с индикаторами используемых потоков данных об угрозах.
3. Служба Kaspersky CyberTrace генерирует оповещения в указанном формате, который содержит индикаторы обнаружения киберугроз на основе входящих событий и записей в потоках данных об угрозах, задействованных в процессе обнаружения киберугроз.
4. Служба Kaspersky CyberTrace отправляет сгенерированные оповещения на указанные адрес и порт.

Управление Kaspersky CyberTrace Service

В этом разделе описывается порядок управления Kaspersky CyberTrace Service.

Управление Kaspersky CyberTrace Service посредством systemd (Linux)

Kaspersky CyberTrace Service можно управлять посредством systemd.

Для управления Kaspersky CyberTrace Service можно использовать все стандартные команды systemd.

Проверка статуса службы

Для проверки статуса Kaspersky CyberTrace Service используется следующая команда:

```
systemctl status cybertrace.service
```

Запуск, остановка и перезапуск службы

Для запуска Kaspersky CyberTrace Service используется следующая команда:

```
systemctl start cybertrace.service
```

> Служба Kaspersky CyberTrace начинает получать события только после загрузки потоков данных об угрозах в память и отправки оповещения KL_ALERT_ServiceStarted.

Для остановки Kaspersky CyberTrace Service используется следующая команда:

```
systemctl stop cybertrace.service
```

Для перезапуска Kaspersky CyberTrace Service используется следующая команда:

```
systemctl restart cybertrace.service
```

Добавление и удаление службы из списка служб, загружаемых при загрузке системы

По умолчанию Kaspersky CyberTrace Service загружается при загрузке системы. Это поведение можно изменить с помощью следующих команд.

Для добавления Kaspersky CyberTrace Service в список служб, загружаемых при загрузке системы, используется следующая команда:

```
systemctl enable cybertrace.service
```

Для удаления Kaspersky CyberTrace Service из списка служб, загружаемых при загрузке системы, используется следующая команда:

```
systemctl disable cybertrace.service
```

Управление Kaspersky CyberTrace Service посредством SCM (Windows)

При установке Kaspersky CyberTrace в операционную систему добавляется несколько служб (см. раздел Установка в ОС Windows).

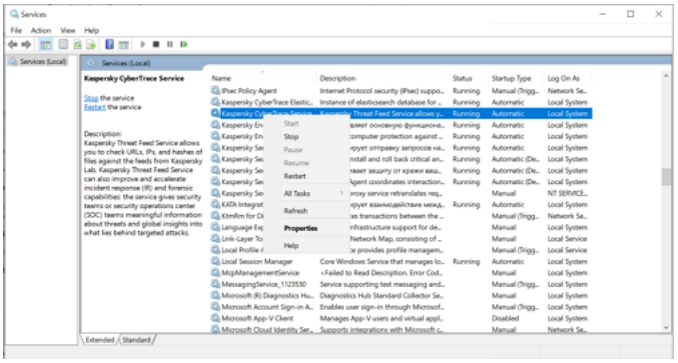
Управление Kaspersky CyberTrace Service посредством графического интерфейса пользователя SCM (Windows)

Чтобы управлять Kaspersky CyberTrace Service с помощью графического интерфейса пользователя SCM, выполните следующие действия:

1. Выполните одно из следующих действий: нажмите **WIN+R**, откройте поле **Поиск** в **меню Пуск** или откройте командную строку Windows.

2. Введите `services.msc` и нажмите клавишу **Enter**.

   Откроется окно **Службы**. В этом окне отображается список всех служб, зарегистрированных в Windows. Текущий статус службы отображается в столбце **Состояние**.



Окно «Службы»

3. Щелкните правой кнопкой мыши по службе «Kaspersky CyberTrace Service», затем в открывшемся контекстном меню выберите запуск, остановку или перезапуск службы.

Управление Kaspersky CyberTrace Service посредством SCM из командной строки

Службами Kaspersky CyberTrace также можно управлять с помощью командной строки Windows и утилиты SC.

Для просмотра состояния службы используется следующая команда:

```
sc query cybertrace
```

Для остановки службы используется следующая команда:

```
sc stop cybertrace
```

Для запуска службы используется следующая команда:

```
sc start cybertrace
```

Для перезапуска службы используются следующие команды:

```
sc stop cybertrace
sc start cybertrace
```

Справка по конфигурационному файлу Kaspersky CyberTrace Service

В этом разделе описывается конфигурационный файл Kaspersky CyberTrace Service.

Рекомендуется настраивать Kaspersky CyberTrace Service на вкладке **Параметры → Служба**. Используйте этот раздел только для настройки параметров, которые нельзя настроить в веб-интерфейсе.

О конфигурационном файле (Kaspersky CyberTrace Service)

Kaspersky CyberTrace Service считывает настройки из конфигурационного файла.

Редактирование конфигурационного файла

Если конфигурационный файл отсутствует или не соответствует правилам, указанным в этом разделе, Kaspersky CyberTrace Service не запускается и выводит сообщение об ошибке.

Чтобы избежать возможных проблем, создайте резервную копию конфигурационного файла Kaspersky CyberTrace Service, прежде чем вносить в него какие-либо изменения. Если после перенастройки Kaspersky CyberTrace Service Kaspersky CyberTrace не работает должным образом, замените конфигурационный файл его резервной копией.

Применение изменений, внесенных в конфигурационный файл

Чтобы изменения вступили в силу, после редактирования конфигурационного файла, необходимо перезагрузить конфигурационный файл или перезапустить Kaspersky CyberTrace Service.

Изменения, внесенные в некоторые элементы конфигурационного файла, можно применить путем перезагрузки конфигурационного файла без перезапуска Kaspersky CyberTrace Service.

Речь идет о следующих элементах:

- `InputSettings > RegExps`
- `Feeds`
- `OutputSettings > RecordFieldContextFormat`
- `OutputSettings > AlertFormat`
- `OutputSettings > EventFormat`

Чтобы перезагрузить конфигурационный файл без перезапуска Kaspersky CyberTrace Service,

запустите сценарий для управления Kaspersky CyberTrace Service с параметром `reloadconfig`.

Чтобы применить изменения, внесенные в другие элементы конфигурационного файла, необходимо перезапустить Kaspersky CyberTrace Service.

Чтобы перезагрузить Kaspersky CyberTrace Service, выполните одно из следующих действий:

- В Linux запустите скрипт `systemctl` для управления Kaspersky CyberTrace Service с параметром `restart`.
- В Windows используйте графический интерфейс пользователя SCM или дважды запустите утилиту SC из командной строки: сначала с параметром `stop cybertrace`, а затем с параметром `start cybertrace`.

Расположение конфигурационного файла (Linux)

В Linux конфигурационный файл, используемый Kaspersky CyberTrace Service, можно указать следующими способами:

- Если Kaspersky CyberTrace Service запускается из командной строки, путь к конфигурационному файлу можно указать в качестве аргумента. По умолчанию задан путь `../etc/kl_feed_service.conf`.
- Когда для управления Kaspersky CyberTrace Service используется скрипт, путь к конфигурационному файлу указывается в параметрах скрипта. По умолчанию задан путь `%service_dir%/etc/kl_feed_service.conf`.

Расположение конфигурационного файла (Windows)

Конфигурационный файл, используемый Kaspersky CyberTrace Service, имеет имя `kl_feed_service.conf` и располагается в том же каталоге, что и бинарный файл Kaspersky CyberTrace Service.

Чувствительность к регистру

Все имена, используемые в конфигурационном файле (например, имена шаблонов или поля потоков данных об угрозах), чувствительны к регистру.

Использование специальных символов

Если в регулярных выражениях и других параметрах требуется использовать специальные символы (например, амперсанд или угловые скобки), текст таких элементов необходимо заключить в раздел CDATA.

В следующем примере параметры заключаются в фигурные скобки:

```
<RecordFieldContextFormat><![CDATA[{%ParamName%=%ParamValue%}]]></RecordFieldContextFormat>
```

EULA

Указывает, были ли приняты условия Лицензионного соглашения (EULA).

Атрибуты

У этого элемента нет атрибутов.

Возможные значения

Этот элемент может иметь следующие значения.

Возможные значения элемента «EULA»

Значение	Описание
`accepted`	Пользователь принял условия Лицензионного соглашения (EULA).
`rejected`	Пользователь не принял условия Лицензионного соглашения (EULA). В этом случае использование Kaspersky CyberTrace невозможно.

Пример

Ниже приведен пример элемента *EULA*.

```
<EULA>accepted</EULA>
```

IndicatorDatabaseSettings

Определяет настройки базы данных индикаторов.

Путь

`IndicatorDatabaseSettings`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- *ConnectionString*

  Задает IP-адрес и порт, которые будут использоваться для доступа к базе данных индикаторов.

  Дополнительные сведения об этом элементе приведены в подразделе «IndicatorDatabaseSettings > ConnectionString» ниже.

IndicatorDatabaseSettings > ConnectionString

Этот элемент должен содержать строку, состоящую из IP-адреса и порта. См. пример ниже.

Этот элемент является обязательным.

Пример

Ниже приведен пример этого элемента.

```
<IndicatorDatabaseSettings>
        <ConnectionString>127.0.0.1:9200</ConnectionString>
</IndicatorDatabaseSettings>
```

RetroScan

Содержит настройки ретроспективного сканирования.

Путь

`RetroScan`

Атрибуты

У этого элемента есть следующие атрибуты.

Атрибуты элемента «RetroScan»

Атрибут	Описание
`enabled`	Указывает, включен ли механизм ретроспективного сканирования. Если ретроспективное сканирование включено, задается значение `true`. Если ретроспективное сканирование отключено, задается значение `false`. По умолчанию задано значение `false`. Этот атрибут является обязательным.
`storage_max_size`	Максимальный размер событий (в МБ), сохраняемых для ретроспективной проверки. По умолчанию задано значение `10000`. Этот атрибут является обязательным.
`storage_event_ttl`	Максимальный интервал времени (в днях), в течение которого хранятся события, накапливаемые для ретроспективного сканирования. По умолчанию задано значение `30`. Этот атрибут является обязательным.
`restroscan_result_ttl`	Максимальный интервал времени (в днях), в течение которого хранятся результаты ретроспективного сканирования. По умолчанию задано значение `90`. Этот атрибут является обязательным.
`retroscan_interval`	Частота (в часах) выполнения задач ретроспективного сканирования по расписанию. По умолчанию задано значение `24`. Этот атрибут является обязательным.
`retroscan_task_threads_for_reading`	Количество потоков, которое необходимо выделить для считывания сохраненных событий.
`retroscan_task_threads_for_analysis`	Количество потоков, которые необходимо выделить для обработки событий после считывания.

Detections

Содержит настройки хранилища обнаружений киберугроз.

Путь

`Detections`

Атрибуты

У этого элемента есть следующие атрибуты.

Атрибуты элемента «Detections»

Атрибут	Описание
`save_detects`	Указывает, включено ли сохранение событий обнаружения киберугроз. Если сохранение событий обнаружения киберугроз включено, задается, значение `true`. Если сохранение событий обнаружения киберугроз отключено, задается значение `false`. По умолчанию задано значение `true`. Этот атрибут является обязательным.
`storage_max_size`	Максимальный размер сохраняемых событий обнаружения киберугроз (в МБ). По умолчанию задано значение `0`. Этот атрибут является обязательным.

Поскольку размер сохраненных событий с киберугрозами проверяется раз в час, время от времени ограничение может оказываться превышенным.

LookupSettings

Содержит параметры поиска индикатора.

Путь

```
LookupSettings
```

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- *RegExps*

  Содержит регулярные выражения Boost, которые используются для парсинга индикаторов при различных видах поиска индикаторов.

Пример

Ниже приведен пример этого элемента.

```
<LookupSettings>
    <RegExps>
        ...
    </RegExps>
</LookupSettings>
```

RegExps

Содержит регулярные выражения Boost, которые используются для парсинга индикаторов при выполнении поиска индикаторов разных типов.

Путь

`LookupSettings > RegExps`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующего вложенного элемента:

- *Источник*

  Содержит параметры для отдельного типа поиска индикаторов.

Пример

Ниже приведен пример этого элемента.

```
<LookupSettings>
    <Source id="default">
        ...
    </Source>
    <Source id="ExampleSource1">
        ...
    </Source>
    <Source id="ExampleSource2">
        ...
    </Source>
</LookupSettings>
```

Получение статистики по данным, получаемым через общедоступные API с помощью методов поиска, требует дополнительных вычислительных ресурсов. Чтобы избежать снижения производительности, можно отредактировать раздел `<Source id="api_single_lookup">` конфигурационного файла `kl_feed_service.conf` и изменить регулярные выражения на `(.*)`. Это, однако, может привести к неправильному расчету статистики.

Раздел `LookupSettings` содержит исходный код `api_single_lookup` со следующими регулярными выражениями:

```
<Source id="api_single_lookup">

<RE_IP type="IP" extract="all" use_for_retroscan="true">(^(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)$)
</RE_IP>

<RE_MD5 type="MD5" extract="all" use_for_retroscan="true">(^[\da-fA-F]{32}$)</RE_MD5>

<RE_SHA1 type="SHA1" extract="all" use_for_retroscan="true">(^[\da-fA-F]{40}$)</RE_SHA1>

<RE_SHA256 type="SHA256" extract="all" use_for_retroscan="true">(^[\da-fA-F]{64}$)</RE_SHA256>

<RE_URL type="URL" extract="all" use_for_retroscan="true"><![CDATA[((?:\S+(?::\S*)?+@)?(?:(?:(?:[a-z\x{00a1}-\x{ffff}0-9]+-*)*[a-z\x{00a1}-
\x{ffff}0-9]*)(?:\.(?:[a-z\x{00a1}-\x{ffff}0-9]+-)*+[a-z\x{00a1}-\x{ffff}0-9]++)*(?:\.(?:[a-z\x{00a1}-\x{ffff}\-0-9]+)))(?:\.*:\d{2,5})?+(?:\.*\/[^\s\"\
<>]*+)?+)]]></RE_URL>

</Source>
```

Чтобы повысить производительность, замените все регулярные выражения на (`.*`) и установите для `use_for_retroscan` значение `false`: _

```
<RE_IP type="IP" extract="all" use_for_retroscan="false">(.\*)</RE\_IP>

<RE_MD5 type="MD5" extract="all" use_for_retroscan="false">(.\*)</RE\_MD5>

<RE_SHA1 type="SHA1" extract="all" use_for_retroscan="false">(.\*)</RE\_SHA1>

<RE_SHA256 type="SHA256" extract="all" use_for_retroscan="false">(.\*)</RE\_SHA256>

<RE_URL type="URL" extract="all" use_for_retroscan="false">(.\*)</RE\_URL>
```

RegExps > Source

Содержит параметры для отдельного типа поиска индикаторов.

Существует два типа поиска индикаторов: `http_single_lookup` (`<Source id="http_single_lookup">`) и `http_file_lookup` (`<Source id="http_file_lookup">`).

Правила для типа поиска индикаторов `http_single_lookup` используются при поиске отдельных значений с помощью веб-интерфейса Kaspersky CyberTrace.

Правила для типа поиска индикаторов `http_file_lookup` используются при поиске хешей указанных файлов или индикаторов в файлах журналов с помощью веб-интерфейса Kaspersky CyberTrace. Поэтому, если требуется найти значения, содержащиеся в файле журнала, имеющем особенный формат, рекомендуется задавать правила для типа поиска индикаторов `http_file_lookup`.

> Если конфигурационный файл содержит тип поиска индикаторов `http_single_lookup` или `http_file_lookup`, настоятельно рекомендуется не удалять регулярные выражения, указанные в этих типах поиска индикаторов по умолчанию, а вместо этого изменять их в соответствии с требованиями.

Путь

`LookupSettings > RegExps > Source`

Атрибуты

У этого элемента есть следующие атрибуты.

Атрибуты элемента «Source»

Атрибут	Описание
`id`	Уникальный идентификатор типа поиска индикатора: `http_single_lookup` или `http_file_lookup`.

Вложенные элементы

Этот элемент является контейнером для вложенных элементов, задающих регулярные выражения для каждого типа индикатора (например, IP-адрес или хеш MD5).

Пример

Ниже приведен пример этого элемента.

```
<Source id="http_single_lookup">
    <RE_IP type="IP" extract="all">(.*)</RE_IP>
    <RE_MD5 type="MD5" extract="all">(.*)</RE_MD5>
    <RE_SHA1 type="SHA1" extract="all">(.*)</RE_SHA1>
    <RE_SHA256 type="SHA256" extract="all">(.*)</RE_SHA256>
    <RE_URL type="URL" extract="all">(.*)</RE_URL>
</Source>
```

Feeds

Определяет, как события должны сверяться с потоками данных об угрозах.

Путь

`Feeds`

Атрибуты

У этого элемента есть следующие атрибуты:

Атрибуты элемента «Feeds»

Атрибут	Описание
`per_scan_detect_limit`	Этот атрибут указывает, сколько раз поле события может быть сопоставлено с потоками данных. Например, определенный URL может соответствовать нескольким записям потока данных об угрозах, поэтому будет сформировано несколько событий обнаружений киберугроз. Атрибут `per_scan_detect_limit` используется для ограничения количества генерируемых событий. Этот атрибут не является обязательным. Если атрибут не указан, количество генерируемых событий не ограничено.
`update_frequency`	Этот атрибут указывает интервал обновления потоков данных об угрозах (в минутах). Можно использовать одно из следующих значений: `0`, `30`, `60`, `120`, `240`, `480`, `960` или `1440`. Значение `0` означает, что Kaspersky CyberTrace не обновляет потоки данных об угрозах автоматически. Этот атрибут не является обязательным. Если атрибут не указан, по умолчанию используется значение `30`.

Вложенные элементы

Этот элемент является контейнером для следующего вложенного элемента:

- *Feed*

  Каждый элемент *Feed* описывает один потока данных об угрозах.

  Конфигурационный файл должен содержать хотя бы один элемент *Feed*.

Пример

Ниже приведен пример этого элемента.

```
<Feeds per_scan_detect_limit="10000" update_frequency="30">
    <Feed filename="Demo_Botnet_CnC_URL_Data_Feed.json" enabled="true" confidence="100">
        ...
    </Feed>
    <Feed filename="Demo_Malicious_Hash_Data_Feed.json" enabled="true" confidence="100">
        ...
    </Feed>
    <Feed filename="Demo_IP_Reputation_Data_Feed.json" enabled="true" confidence="100">
        ...
    </Feed>
</Feeds>
```

Feed

Описывает поток данных об угрозах или источник данных об угрозах.

Путь

`Feeds > Feed`

Атрибуты

У этого элемента есть следующие атрибуты:

Атрибуты элемента «Feed»

Атрибут	Описание
`enabled`	Указывает, включен ли поток данных об угрозах или источник данных об угрозах на глобальном уровне (для всех тенантов).
`filename`	Имя источника данных об угрозах или имя файла потока данных об угрозах в каталоге, указанном в элементе `ServiceSettings` → `Bases`. Этот атрибут является обязательным.
`confidence`	Уровень доверия к потоку данных об угрозах или источнику данных об угрозах. Можно использовать значения в диапазоне от `1` до `100`. По умолчанию заданы значения: `100` для потоков данных об угрозах «Лаборатории Касперского», `50` для потоков данных об угрозах OSINT и `50` для сторонних потоков или источников данных об угрозах. Этот атрибут является обязательным.

Атрибут	Описание
`outdated_alert_period`	Время (в часах) с момента последнего обновления потока данных об угрозах, по истечении которого в место назначения события отправляется уведомление об устаревшем потоке данных об угрозах (`KL_ALERT_OutdatedFeed`). По умолчанию для этого параметра задано значение `0`, т. е. уведомления об устаревших потоках данных не отправляются. Если атрибут не указан, используется значение элемента `ServiceSettings` > `OutdatedBasesAlertPeriod`. Рекомендуется установить значение `120` для коммерческих потоков данных об угрозах Kaspersky Data Feed и `720` для потоков данных о постоянных угрозах повышенной сложности (APT). Также рекомендуется для потоков данных об угрозах OSINT установить для этого параметра значение `0` или другое целесообразное значение. Для сторонних источников данных об угрозах этот параметр по умолчанию имеет значение `0`. Этот атрибут не является обязательным.
`indicator_lifetime`	Время (в минутах), по истечении которого индикаторы компрометации потока данных об угрозах или источника данных об угрозах удаляются из базы данных. Если индикатор обнаруживается на основе входящего события, он не удаляется из базы данных, но больше не может использоваться в процессе сопоставления для потока данных об угрозах, содержащего этот индикатор, или источника данных об угрозах, который его предоставляет. Чтобы снять ограничение по времени для аннулирования потока или источника данных об угрозах, установите для этого атрибута значение `0`. По умолчанию значение этого атрибута равно семи дням (10080 минутам). Этот атрибут применяется к источникам, отличным от Kaspersky Threat Data Feeds.
`vendor`	Название поставщика потока данных об угрозах или источника данных об угрозах. Этот атрибут не является обязательным.
`use_for_retroscan`	Указывает, следует ли использовать индикаторы из потока данных или источника данных об угрозах для ретроспективного сканирования. Если индикаторы должны использоваться для ретроспективного сканирования, для этого атрибута задается значение `true`. Если индикаторы не должны использоваться для ретроспективного сканирования, для этого атрибута задается значение `false`.
`is_restapi`	Указывает, что источник данных об угрозах был добавлен с помощью REST API. Если источник данных об угрозах был добавлен с помощью REST API, значение этого атрибута — `true`. Этот атрибут не является обязательным.

Пример

Ниже приведен пример этого элемента.

```
<Feed filename="Demo_Botnet_CnC_URL_Data_Feed.json" vendor="Kaspersky" confidence="100" indicator_lifetime="0"
enabled="true" use_for_retroscan="false"/>
```

ServiceSettings

Задает параметра процесса Kaspersky CyberTrace Service.

Путь

`ServiceSettings`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- *FeedUtil*

  Содержит параметры Feed Utility.

- *BasesSettings*

  Содержит параметры потоков данных.

- *ScanSettings*

  Содержит параметры сканера.

- *HTTPServer*

  Содержит параметры HTTP-службы Kaspersky CyberTrace.

- *Security*

  Содержит параметры безопасности.

- *FeedsRollbackEnabled*

  Указывает, включен или выключен откат потоков данных об угрозах.

  Если включен откат потоков данных об угрозах, откат потоков данных об угрозах выполняется в случае, если Kaspersky CyberTrace не сможет загрузить новые индикаторы в Matching engine после обновления потоков данных об угрозах. Kaspersky CyberTrace удаляет новые индикаторы из базы данных и использует предыдущую версию потоков данных об угрозах.

  Возможные значения:

  - `true` — откат потоков данных об угрозах включен.
  - `false` — откат потоков данных об угрозах отключен.

  Kaspersky CyberTrace считывает элемент *FeedsRollbackEnabled* только во время инициализации и в дальнейшем не считывает его повторно.

  По умолчанию элемент *FeedsRollbackEnabled* в файле конфигурации отсутствует. Если этот элемент отсутствует, откат потоков данных об угрозах включен.

- *Audit*

  Содержит параметры аудита действий пользователей.

Пример

Ниже приведен пример этого элемента.

```
<ServiceSettings>
    <FeedUtil>
        ...
    </FeedUtil>
    <BasesSettings>
        ...
    </BasesSettings>
    <ScanSettings>
        ...
    </ScanSettings>
    <HTTPServer>
        ...
    </HTTPServer>
    <FeedsRollbackEnabled>true</FeedsRollbackEnabled>
    <Audit>
        ...
    </Audit>
</ServiceSettings>
```

FeedUtil

Содержит параметры Feed Utility.

Путь

`ServiceSettings > FeedUtil`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующего вложенного элемента:

- *ConfigurationPath*

  Путь к конфигурационному файлу Feed Utility.

  Этот элемент является обязательным.

Пример

Ниже приведен пример этого элемента.

```
<FeedUtil>
    <ConfigurationPath>../etc/kl_feed_util.conf</ConfigurationPath>
</FeedUtil>
```

BasesSettings

Содержит параметры потоков данных.

Путь

`ServiceSettings > BasesSettings`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- *Bases*

  Задает путь к каталогу, в котором находятся потоки данных об угрозах «Лаборатории Касперского». Если задан относительный путь, он вычисляется относительно каталога, в котором находится бинарный файл службы.

  Этот элемент является обязательным.

- *BasesBackup*

  Задает путь к каталогу, в котором находятся резервные версии потоков данных «Лаборатории Касперского». Если задан относительный путь, он вычисляется относительно каталога, в котором находится бинарный файл службы.

  Этот элемент является обязательным.

- *BasesDownload*

  Задает путь к каталогу, в котором находятся потоки данных, скачанные у «Лаборатории Касперского». Если задан относительный путь, он вычисляется относительно каталога, в котором находится бинарный файл службы.

  Этот элемент является обязательным.

- *OutdatedBasesAlertPeriod*

  Интервал времени (в часах) с момента последнего обновления потока данных об угрозах, по истечении которого в место назначения события отправляется уведомление об устаревшем потоке данных об угрозах. Чтобы отключить уведомления, задайте для этого параметра значение `0`. Этот параметр учитывается для всех потоков данных об угрозах, у которых нет атрибута *outdated_alert_period*.

  Этот элемент не является обязательным. Если он не указан, используется значение по умолчанию `0`.

Пример

Ниже приведен пример этого элемента.

```
<BasesSettings>
    <Bases>../feeds</Bases>
    <BasesBackup>../feeds/backup</BasesBackup>
    <BasesDownload>../feeds/download</BasesDownload>
    <OutdatedBasesAlertPeriod>120</OutdatedBasesAlertPeriod>
    <ScannersCount>9</ScannersCount>
</BasesSettings>
```

ScanSettings

Содержит параметры сканера.

Путь

`ServiceSettings > ScanSettings`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- *ScannersCount*

  Количество сканеров. Каждый сканер работает с одним TCP-соединением.

  При изменении этой конфигурации следует указать один сканер в дополнение к количеству сканеров, необходимых для самого Kaspersky CyberTrace. Это необходимо для механизма проверки работоспособности.

  Этот элемент не является обязательным. Если он не указан, используется значение по умолчанию `9`.

  Мы рекомендуем использовать значение по умолчанию. При необходимости значение по умолчанию можно увеличить. Максимальное возможное значение составляет `20`.

- *ScanningThreadsPerScanner*

  Количество потоков на сканер.

  Этот элемент не является обязательным. Если он не указан, используется значение по умолчанию `8`.

- *EPSLimit*

  Параметры порогового EPS системы.

  Дополнительные сведения об этом элементе приведены в подразделе "ScanSettings > EPSLimit" ниже.

ScanSettings > EPSLimit

Задает параметры порогового EPS системы.

Этот элемент является обязательным. Значение по умолчанию: `<EPSLimit enabled="false">50000</EPSLimit>`.

Элемент может принимать значения в диапазоне от `1` до `199999`.

У этого элемента есть следующие атрибуты:

Атрибуты элемента «EPSLimit»

Атрибут	Описание
`enabled`	Определяет, управляет ли Kaspersky CyberTrace пороговым EPS системы. Возможные значения: `true`, `false`. Если задано значение `true`, то осуществляется управление пороговым EPS системы. Если значение равно `false`, управление пороговым EPS системы не осуществляется. В таком случае не исключено неожиданное снижение производительности системы.

Пример

Ниже приведен пример этого элемента.

```
<ScanSettings>
    <ScannersCount>9</ScannersCount>
    <ScanningThreadsPerScanner>8</ScanningThreadsPerScanner>
    <EPSLimit enabled="false">50000</EPSLimit>
</ScanSettings>
```

Security

Содержит параметры безопасности.

Путь

`ServiceSettings > Security`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- *TLS*

  Задает путь к сертификату и закрытому ключу.

  - *SSLCertificatePath*

    Путь к сертификату в формате PEM на локальном сервере для HTTPS-соединений. Если указан относительный путь, он отсчитывается относительно исполняемого файла.

    > По соображениям безопасности не храните свой сертификат в папке общего доступа, доступной по сети, и не указывайте путь к сетевой папке общего доступа, содержащей сертификат.

    Этот элемент не является обязательным. Если он не указан, используется файл `../httpsrv/kl_feed_service_cert.pem`.

  - *SSLPrivateKeyPath*

    Путь к закрытому ключу в формате PEM на локальном сервере для HTTPS-соединений. Если указан относительный путь, он отсчитывается относительно исполняемого файла.

    > По соображениям безопасности не храните свой закрытый ключ в папке общего доступа, доступной по сети, и не указывайте путь к сетевой папке общего доступа, содержащей закрытый ключ.

    Этот элемент не является обязательным. Если он не указан, используется файл `../httpsrv/kl_feed_service_private.pem`.

- *CustomFeedsSecurity*

  Указывает путь к директориям, к которым разрешен доступ, с пользовательскими потоками данных.

- *LogoutTimeout*

  Параметры выхода пользователя из системы.

  Элемент может принимать значения в диапазоне от 1 до 480.

  У этого элемента есть следующие атрибуты:

  Атрибуты элемента «LogoutTimeout»

Атрибут	Описание
`enabled`	Определяет, продлевается ли сеанс неограниченно долго при неактивности пользователя. Возможные значения: `true`, `false`. Если задано значение `true`, сеанс пользователя продлевается неограниченно долго. Если задано значение `false`, необходимо указать период обновления сеанса пользователя.

Примеры

Пример элемента *TLS*:

```
<Configuration>
        <ServiceSettings>
                <Security>
                        <TLS>
                             <SSLCertificatePath>../httpsrv/kl_feed_service_cert.pem</SSLCertificatePath>
                             <SSLPrivateKeyPath>../httpsrv/kl_feed_service_private.pem</SSLPrivateKeyPath>
                        </TLS>
                        ...
                </Security>
        </ServiceSettings>
</Configuration>
```

Пример элемента *LogoutTimeout*:

```
<ServiceSettings>
        <Security>
                ...
                <LogoutTimeout enabled="false">5</LogoutTimeout>
        </Security>
</ServiceSettings>
```

CustomFeedsSecurity

Содержит разрешенные каталоги для пользовательских потоков данных.

Путь

`Security > CustomFeedsSecurity`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- *AllowedDirectories*
- *Путь*

Этот элемент хранит каталог для пользовательских потоков данных, который выбран по умолчанию или разрешен пользователем.

Каталог по умолчанию для Windows: `%path%/Kaspersky CyberTrace/custom_feeds`.

Каталог по умолчанию для Linux: `%path%/ktfs/custom_feeds`.

`%path%` – это абсолютный путь к каталогу, содержащему каталог CyberTrace.

Примеры

Пример элемента *CustomFeedsSecurity*:

```
<Configuration>
        <ServiceSettings>
                <Security>
                        <CustomFeedsSecurity>
                                <AllowedDirectories>
                                        ...
                                    <Path>C:\Program Files\Kaspersky Lab\Kaspersky CyberTrace\custom_feeds</Path>
                                <Path>\\FileCluster01\Security\CustomFeeds</Path>
                                <Path>D:\FeedData\</Path>
                                        ...
                                </AllowedDirectories>
                        </CustomFeedsSecurity>
                </Security>
        </ServiceSettings>
</Configuration>
```

HTTPServer

Содержит параметры HTTP-службы Kaspersky CyberTrace.

Путь

`ServiceSettings > HTTPServer`

Атрибуты

У этого элемента нет атрибутов.

Необязательный

Этот элемент не является обязательным. Если он не указан, используются значения по умолчанию.

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- *ConnectionString*

  Задает IP-адрес и порт, по которым доступен HTTP-службы Kaspersky CyberTrace.

  В этом элементе можно указать адрес IPv4 или IPv6.

  Этот элемент не является обязательным. Если он не указан, используются IP-адрес и порт `127.0.0.1:443`. После завершения процесса установки для элемента *HTTPServer > ConnectionString* по умолчанию задано значение `0.0.0.0:443`.

- *ResourcesIP*

Содержит IP-адрес или имя хоста, которые используются в поле `%IndicatorInfo%` оповещений об обнаружении индикаторов компрометации, в служебных оповещениях для уведомления о завершении ретроспективного сканирования и в результатах экспорта индикатора.

В этом элементе можно указать адрес IPv4 или IPv6.

Этот элемент является обязательным. По умолчанию указано значение `127.0.0.1`.

> Вместо локального IP-адреса желательно указать сетевой IP-адрес хоста.

- *TemplatesPath*

  Путь к каталогу, содержащему страницы макета для HTTP-службы Kaspersky CyberTrace. Если указан относительный путь, он отсчитывается относительно исполняемого файла.

  Этот элемент не является обязательным. Если он не указан, используется каталог `../httpsrv/templates/`.

Пример

Ниже приведен пример этого элемента.

```
<HTTPServer>
    <ConnectionString>0.0.0.0:443</ConnectionString>
    <ResourcesIP>127.0.0.1</ResourcesIP>
    <TemplatesPath>../httpsrv/templates</TemplatesPath>
</HTTPServer>
```

Audit

Содержит параметры аудита действий пользователей.

Путь

`Configuration` → `ServiceSettings` → `Audit`.

Атрибуты

У этого элемента есть атрибут `enabled`, который указывает, включен ли аудит действий пользователей. Этот атрибут может иметь следующие значения:

- `true` – аудит действий пользователей включен.
- `false` – аудит действий пользователей отключен.

По умолчанию задано значение `true`. Этот атрибут является обязательным.

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- `Retention` – срок хранения событий действий пользователя. Этот элемент содержит атрибут `enabled`, который может иметь следующие значения:
  - `true` – задан срок хранения в определенное число дней. Если для атрибута `enabled` задано значение `true`, элемент `Retention` должен содержать определенное числовое значение.
  - `false` – срок хранения не ограничен.

  По умолчанию `Retention` содержит атрибут `enabled="true"` и равен 90 дням.
- `AuditStoragePath` – путь к каталогу с файлами журнала аудита действий пользователей.

Пример

Ниже приведен пример этого элемента.

```
<Audit enabled="true">
        <Retention enabled="true">365</Retention>
        <AuditStoragePath>%path%/ktfs/var/audit</AuditStoragePath>
</Audit>
```

AuthenticationServers

Задает настройки подключения к серверам LDAP.

Путь

`AuthenticationServers`

Атрибуты

У этого элемента нет атрибутов.

Обязательный

Этот элемент является обязательным.

Вложенные элементы

Этот элемент является контейнером для следующего вложенного элемента:

- *AuthenticationServer*

  Содержит параметры настройки соединения LDAP.

Пример

Ниже приведен пример этого элемента.

```
<AuthenticationServers>
    <AuthenticationServer type="LDAP" enabled="true">
            ...
    </AuthenticationServer>
</AuthenticationServers>
```

AuthenticationServers > AuthenticationServer

Содержит параметры настройки соединения LDAP.

Путь

`AuthenticationServers > AuthenticationServer`

Необязательный

Этот элемент не является обязательным.

Атрибуты

У этого элемента есть следующие атрибуты.

Атрибуты элемента «AuthenticationServer»

Атрибут	Описание
`type`	Указывает тип сервера для подключения. Возможные значения: `LDAP`. Этот атрибут является обязательным.
`enabled`	Указывает, должен ли использоваться заданный сервер. Возможные значения: `true`, `false`. Этот атрибут является обязательным.

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- *ConnectionString*

Содержит параметры подключения к серверу LDAP.

Дополнительную информацию об этом элементе см. в подразделе «AuthenticationServer > ConnectionString» ниже.

- *DomainName*

  Путь к базе данных, содержащей учетные записи пользователей, которым разрешен доступ к Kaspersky CyberTrace.

  Дополнительную информацию об этом элементе см. в подразделе «AuthenticationServer > DomainName» ниже.

- *AdministratorAccountsFilter*

  Содержит правила фильтрации для учетных записей пользователей, которым должна быть назначена роль «Администратор».

  Элемент *AdministratorAccountsFilter* не должен содержать значение, указанное в элементе *AnalystAccountsFilter*.

  Элемент *AdministratorAccountsFilter* может быть пустым. Если это значение не задано, пользователи не могут осуществлять вход посредством аутентификации LDAP и получать роль «Администратор».

- *AnalystAccountsFilter*

  Содержит правила фильтрации для учетных записей пользователей, которым должна быть назначена роль «Аналитик».

  Элемент *AnalystAccountsFilter* не должен содержать значение, указанное в элементе *AdministratorAccountsFilter*.

  Элемент *AnalystAccountsFilter* может быть пустым. Если это значение не задано, пользователи не могут осуществлять вход посредством аутентификации LDAP и получать роль «Аналитик».

  Этот элемент является обязательным.

AuthenticationServer > ConnectionString

IP-адрес или полное доменное имя (FQDN) и порт сервера LDAP.

Этот элемент является обязательным и не может быть пустым.

У этого элемента есть следующие атрибуты.

Атрибуты элемента «ConnectionString»

Атрибут	Описание
`use_encryption`	Указывает, необходимо ли использовать SSL/TLS или STARTTLS-соединение. Если используется SSL/TLS-соединение, задается значение `ssl/tls`. Если используется STARTTLS-соединение, задается значение `starttls`. Если протокол шифрования не используется, задается значение `none`.
`connection_timeout`	Задает время ожидания ответа от сервера LDAP в секундах. Диапазон значений этого атрибута: от `1` до `60`.

AuthenticationServer > DomainName

Путь к базе данных, содержащей учетные записи пользователей, которым разрешен доступ к Kaspersky CyberTrace.

Этот элемент является обязательным и не может быть пустым.

У этого элемента есть следующие атрибуты.

Атрибуты элемента «DomainName»

Атрибут	Описание
`use_principal_name`	Указывает, используется ли формат User Principal Name (UPN). Если требуется использовать UPN, необходимо указать значение `true`. В противном случае следует указать значение `false`. В этом случае используется формат имени учетной записи SAM.

Пример

Ниже приведен пример этого элемента.

```
<AuthenticationServer type="LDAP" enabled="true">
    <ConnectionString use_encryption="false" connection_timeout="20">ldap.example.com:389</ConnectionString>
    <DomainName use_principal_name="true">dc=testing,dc=con</DomainName>
    <AdministratorAccountsFilter>cn=theadministrator</AdministratorAccountsFilter>
    <AnalystAccountsFilter>cn=users_an</AnalystAccountsFilter>
</AuthenticationServer>
```

NotificationSettings

Содержит параметры отправки служебных оповещений (исходящих оповещений, информирующих другое программное обеспечение (например, SIEM-систему) о состоянии Kaspersky CyberTrace Service) и оповещений об обнаружении индикаторов компрометации (исходящих оповещений, содержащих информацию об обнаруженных сопоставлениях с индикаторами).

Определяет адрес и порт целевого программного обеспечения, в которое отправляются оповещения, а также формат оповещений.

Путь

`NotificationSettings`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- *EventSettings*

  Задает параметры исходящих служебных оповещений и оповещений об обнаружении индикаторов компрометации.

Этот элемент является обязательным.

- *ServiceAlertsSettings*

  Задает параметры подключения к программному обеспечению, в которое отправляются события, для отправки служебных оповещений.

  Этот элемент является обязательным.

- *AuditAlertsSettings*

  Содержит параметры для отправки событий аудита действий пользователей в другие программы по протоколу TCP.

Ниже приведен пример этого элемента.

```
<NotificationSettings>
    <EventSettings>
        ...
    </EventSettings>
    <ServiceAlertsSettings>
        ...
    </ServiceAlertsSettings>
    <AuditAlertsSettings>
        ...
    </AuditAlertsSettings>
</NotificationSettings>
```

EventSettings

Задает параметры исходящих служебных оповещений и оповещений об обнаружении индикаторов компрометации.

Путь

`NotificationSettings > EventSettings`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- *EventSendingRetriesCount*

  Количество попыток, предпринимаемых службой Kaspersky CyberTrace для повторной отправки оповещений об обнаружении индикаторов компрометации в SIEM-систему, если первая попытка отправки не удалась. Если значение `EventSendingRetriesCount` равно `0`, служба Kaspersky CyberTrace отправляет каждое оповещение об обнаружении индикаторов компрометации один раз и не пытается отправить его повторно.

  Максимально возможное значение равно `10`. По умолчанию задано значение `3`.

  Этот элемент является обязательным.

- *EventSendingRetriesTimeout*

Интервал времени в секундах между попытками, предпринимаемыми Kaspersky CyberTrace Service для повторной отправки оповещения об обнаружении индикаторов компрометации в SIEM-систему. Максимально возможное значение равно `60`.

Этот элемент является обязательным.

По умолчанию задано значение `10`.

Пример

Ниже приведен пример этого элемента.

```
<ServiceSettings>
    <EventSendingRetriesCount>3</EventSendingRetriesCount>
    <EventSendingRetriesTimeout>10</EventSendingRetriesTimeout>
</ServiceSettings>
```

ServiceAlertsSettings

Задает параметры подключения к программному обеспечению, в которое отправляются события, для отправки служебных оповещений.

Путь

`NotificationSettings > ServiceAlertsSettings`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Чтобы указать значения элементов *AlertFormat* и *ContextFormat*, может потребоваться ознакомление с дополнительной информацией о шаблонах формата событий.

Этот элемент является контейнером для следующих вложенных элементов:

- *AlertConnectionString*

  Задает IP-адрес (или хост) и порт, на который служба будет отправлять служебные информационные сообщения.

  Этот элемент не является обязательным.

  Дополнительные сведения об этом элементе приведены в подразделе «OutputSettings > AlertConnectionString» ниже.

- *AlertFormat*

  Задает формат исходящих оповещений, которые информируют целевое программное обеспечение о состоянии службы Kaspersky CyberTrace.

  Этот элемент не является обязательным. Если элемент отсутствует в конфигурационном файле, уведомление не формируется.

- *ContextFormat*

Указывает, как поля контекста должны добавляться к служебному оповещению.

Этот элемент является обязательным.

OutputSettings > AlertConnectionString

Задает IP-адрес (или хост) и порт, на который служба будет отправлять служебные оповещения.

Значение элемента имеет формат `<ip_address>:<port>` (если используются IP-адрес и порт) или `\\.\pipe\<pipe_name>` (если используется именованный канал Windows). IP-адрес должен состоять из четырех десятичных октетов, разделенных точкой. Значение в каждом октете должно быть меньше 256.

Этот элемент не является обязательным. Если элемент пропущен, для этого элемента используется атрибут *enabled* со значением `false`.

У этого элемента есть следующие атрибуты:

Атрибуты элемента «AlertConnectionString»

Атрибут	Описание
`enabled`	Определяет, отправляет ли служба Kaspersky CyberTrace служебные оповещения на указанные IP-адрес и порт. Возможные значения: `true`, `false`. Если значение равно `true`, служба Kaspersky CyberTrace отправляет служебные оповещения на IP-адрес и порт, указанные в этом элементе. Если значение равно `false`, служба Kaspersky CyberTrace отправляет оповещения на IP-адрес и порт, указанные в элементе *OutputSettings → ConnectionString*.

Пример

Ниже приведен пример этого элемента.

```
<ServiceAlertsSettings>
    <AlertConnectionString enabled="true">127.0.0.1:9998</AlertConnectionString>
    <AlertFormat>%Date% alert=%Alert%%RecordContext%</AlertFormat>
    <ContextFormat>%ParamName%=%ParamValue%</ContextFormat>
</ServiceAlertsSettings>
```

AuditAlertsSettings

Содержит параметры для отправки событий аудита действий пользователей в другие программы по протоколу TCP.

Путь

`Configuration` → `NotificationSettings` → `AuditAlertsSettings`.

Атрибуты

У этого элемента нет атрибутов.

Атрибуты

Этот элемент является контейнером для вложенного элемента `AlertConnectionString`.

Элемент `AlertConnectionString` содержит параметры для отправки событий аудита действий пользователя в другие программы (например, в систему SIEM) по протоколу TCP. Значение элемента — строка с IP-адресом или именем хоста и портом программы, в которую будут отправляться события действий пользователей, в формате `<IP-адрес или имя хоста>:<порт>`.

Элемент `AlertConnectionString` содержит атрибуты, описанные в таблице ниже.

Атрибуты `AlertConnectionString`

Атрибут	Описание
`enabled`	Определяет, отправляются ли события действий пользователя в другие программы по протоколу TCP. Возможные значения: • `true` – события действий пользователей отправляются в другие программы по протоколу TCP. • `false` – события действий пользователей не отправляются в другие программы по протоколу TCP и сохраняются только локально.
`use_encryption`	Тип подключения, используемый при отправке событий действий пользователя. Возможные значения: • `TLS` – использование шифрования TLS с проверкой сертификата. • `TLSNoValidation` – использование шифрования TLS без проверки сертификата. • `None` – шифрование TLS не используется.

Пример

Ниже приведен пример этого элемента.

```
<AuditAlertsSettings>
        <AlertConnectionString enabled="true" use_encryption="TLS"><IP-адрес>:<порт></AlertConnectionString>
</AuditAlertsSettings>
```

Domains

Содержит конфигурацию для тенантов.

Путь

`Domains`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующего вложенного элемента:

- *Домен*

Пример

Ниже приведен пример этого элемента.

```
<Domains>
    <Domain name="General">
       ...
    </Domain>
    <Domain name="Tenant1">
       ...
    </Domain>
</Domains>
```

Домен

Определяет конфигурацию для тенанта.

Путь

`Domains > Domain`

Атрибуты

У этого элемента есть следующие атрибуты.

Атрибуты элемента «Domain»

Атрибут	Описание
`name`	Имя тенанта
`id`	Идентификатор тенанта

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- *Описание*

  Описание тенанта.

  Этот элемент не является обязательным.

- *InputSettings*

  Настройки входящего соединения для этого тенанта.

- *OutputSettings*

  Настройки исходящего соединения для этого тенанта.

- *EPSLimit*

  Параметры порогового EPS тенанта.

  Дополнительные сведения об этом элементе приведены в подразделе "Domain > EPSLimit" ниже.

- *Потоки данных*

Настройки потоков данных, используемых в рамках этого тенанта.

Дополнительные сведения об этом элементе приведены в подразделе «Domain > Feeds» ниже.

Domain > EPSLimit

Задает параметры порогового EPS тенанта.

Элемент может принимать значения в диапазоне от `1` до `199999`.

У этого элемента есть следующие атрибуты:

Атрибуты элемента «EPSLimit»

Атрибут	Описание
`enabled`	Определяет, управляет ли Kaspersky CyberTrace пороговым EPS тенанта. Возможные значения: `true`, `false`. Если задано значение `true`, то осуществляется управление пороговым EPS тенанта. Если значение равно `false`, управление пороговым EPS тенанта не осуществляется. Это может повлиять на других тенантов (если таковые имеются).

Domain > Feeds

Настройки потоков данных, используемых в рамках тенанта.

Этот элемент является контейнером для следующего вложенного элемента:

- Feed

  Параметры для определенного потока данных в тенанте.

Пример

Ниже приведен пример этого элемента.

```
<Domain name="CustomDomain">
    <Description>Описание пользовательского домена</Description>
    <InputSettings>
        ...
    </InputSettings>
    <OutputSettings>
        ...
    </OutputSettings>
    <EPSLimit enabled="true">1000</EPSLimit>
    <Feeds>
        ...
    </Feeds>
</Domain>
```

InputSettings

Содержит параметры ввода для тенанта.

Этот элемент задает IP-адрес и порт, которые Kaspersky CyberTrace Service будет прослушивать в ожидании входящие события, правила нормализации для обработки событий и регулярные выражения для парсинга событий.

Путь

```
Domains > Domain > InputSettings
```

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- *RegExps*

  Содержит регулярные выражения Boost, которые используются для парсинга входящих событий из различных источников.

- *ConnectionString*

  Задает IP-адрес и порт (или именованный канал Windows), который служба будет прослушивать в ожидании входящих событий.

- *EventDelimiter*

  Задает правило разделения входящих событий.

Пример

Ниже приведен пример этого элемента.

```
<InputSettings>
    <RegExps>
        ...
    </RegExps>
    <ConnectionString>0.0.0.0:9999</ConnectionString>
</InputSettings>
```

RegExps

Содержит регулярные выражения Boost, которые используются для парсинга входящих событий из разных источников.

Путь

```
Domains > Domain > InputSettings > RegExps
```

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующего вложенного элемента:

- *Источник*

  Содержит параметры для определенного источника событий.

Пример

Ниже приведен пример этого элемента.

```
<RegExps>
    <Source id="default">
        ...
    </Source>
    <Source id="ExampleSource1">
        ...
    </Source>
    <Source id="ExampleSource2">
        ...
    </Source>
</RegExps>
```

Источник

Содержит параметры для определенного источника событий.

Регулярные выражения и правила нормализации событий, задаваемые в конфигурационном файле, группируются по источникам событий, которым соответствуют элементы `Source`. Обычно такими источниками событий являются устройства, выдающие события, которые затем проверяются средствами Kaspersky CyberTrace Service. Каждый элемент `Source` содержит определенный набор правил. В элементе `InputSettings` > `RegExps` может быть один или несколько элементов `Source`.

Обратите внимание, что сначала применяются правила нормализации событий, а затем применяются регулярные выражения.

Особый источник событий

Непременно должен быть определен источник событий по умолчанию с идентификатором «default» (`<Source id="default">`). Правила источника событий по умолчанию имеют более низкий приоритет, чем правила, относящиеся к определенному источнику событий.

Регулярные выражения источника событий `default` для поиска URL, IP-адресов и хешей являются универсальными; т. е. их можно использовать для парсинга событий, выдаваемых большинством устройств. Эти регулярные выражения можно использовать для парсинга событий, содержащих несколько URL, однако нельзя использовать, например, для парсинга событий, содержащих URL без указания протокола. Использование универсальных регулярных выражений снижает производительность Kaspersky CyberTrace Service по сравнению с использованием регулярных выражений для конкретных устройств. Кроме того, универсальные регулярные выражения не обрабатывают разброс различных частей URL в событии (например, хоста и пути). Универсальные регулярные выражения для поиска хешей могут извлекать последовательности символов, которые на самом деле не являются хешами.

Путь

`Domains > Domain > InputSettings > RegExps > Source`

Атрибуты

У этого элемента есть следующие атрибуты.

Атрибуты элемента «Source»

Атрибут	Описание
`id`	Уникальный идентификатор источника событий. События обнаружения киберугроз могут ссылаться на идентификаторы источников событий с помощью выражений вида %SourceId%.
`ip`	IP-адрес источника событий. Если событие пришло из источника события, имеющего указанный IP-адрес, такое событие обрабатывается с использованием правил, содержащихся в данном элементе `Source`. Если IP-адрес источника событий не входит в число тех, что указаны в атрибуте `ip` элементов `Source`, определяется имя хоста источника событий и выполняется поиск элемента `Source`, у которого в атрибуте `hostname` задано это имя хоста. Для обработки события используются правила этого элемента `Source`. Этот атрибут невозможно задать для источника событий `default`.
`hostname`	Имя хоста источника событий. Значение имени хоста извлекается из события. В событиях syslog имя хоста следует за меткой времени (https://tools.ietf.org/html/rfc5424). Например, в событии `Feb 2 11:57:59 sample-hostname alert: sample event text` именем хоста является строка `sample-hostname`. Если событие поступило из источника событий, обладающего указанным именем хоста, а IP-адрес источника событий не входит в число тех, что указаны в атрибуте `ip` элементов `Source`, событие обрабатывается с использованием правил, содержащихся в этом элементе `Source`. Этот атрибут невозможно задать для источника событий `default`.
`regex`	Регулярное выражение, используемое для определения того, поступило ли событие из источника. Заданное регулярное выражение применяется к событию. Если регулярное выражение сопоставляет событие один или несколько раз, считается, что событие поступило из данного источника. В этом случае событие обрабатывается с использованием правил, содержащихся в данном элементе `Source`. Этот атрибут невозможно задать для источника событий `default`.

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- *Регулярные выражения*

  Регулярные выражения, которые используются для парсинга входящих событий из этого источника.

  Каждое регулярное выражение представляет собой отдельный элемент с именем, соответствующим имени регулярного выражения.

- *NormalizingRules*

  Правила изменения входящих событий.

Пример

Ниже приведен пример этого элемента.

```
<Source id="CustomSource" ip="192.0.2.15">
    <RE_MD5 type="MD5" extract="all">([\da-fA-F]{32})</RE_MD5>
    <RE_SHA1 type="SHA1" extract="all">([\da-fA-F]{40})</RE_SHA1>
    <RE_SHA256 type="SHA256" extract="all">([\da-fA-F]{64})</RE_SHA256>
    <NormalizingRules>
        ...
    </NormalizingRules>
</Source>
```

Source > NormalizingRules

Определяет правила изменения входящих событий.

Путь

`Domains > Domain > InputSettings > RegExps > Source > NormalizingRules`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- *Replace*

  Эти элементы задают правила замены.

- *Ignore*

  Эти элементы задают правила игнорирования.

NormalizingRules > Replace

Задает правило замены.

У этого элемента есть следующие атрибуты.

Атрибуты элемента «Replace»

Атрибут	Описание
`input`	Задает регулярное выражение для правила.
`output`	Задает последовательность символов, используемую для замены.

NormalizingRules > Ignore

Задает правило игнорирования

У этого элемента есть следующие атрибуты.

Атрибуты элемента «Ignore»

Атрибут	Описание
`input`	Задает регулярное выражение для правила.

Пример

Ниже приведен пример этого элемента.

```
<NormalizingRules>
    <Replace input="^\<(\d+)\>" output="NEW_EVENT\:\1\s" />
    <Ignore input="Device0002" />
</NormalizingRules>
```

Source > Regular expression

Определяет регулярное выражение для источника событий.

Путь

`Domains > Domain > InputSettings > RegExps > Source > %RegexpName%`

Имя этого элемента совпадает с именем регулярного выражения.

Атрибуты

У этого элемента есть следующие атрибуты.

Атрибуты элемента «%RegexpName%»

Атрибут	Описание
`type`	Задает тип значения, извлекаемого этим регулярным выражением. Возможные значения: • `URL` — URL • `MD5` — хеш MD5 • `SHA1` — хеш SHA1 • `SHA256` — хеш SHA256 • `HASH` — хеш MD5, SHA1 или SHA256 • `IP` — IP-адрес • `DOMAIN` — доменное имя • `CONTEXT` — контекстная информация Этот атрибут не является обязательным. Если он не указан, используется значение `CONTEXT` по умолчанию.
`extract`	Указывает, как именно должны извлекаться множественные значения, совпавшие с регулярным выражением. Возможные значения: `all` и `first`. Значение `all` указывает, что извлекаться должны все значения, совпавшие с регулярным выражением. Для каждого совпавшего значения создается отдельное оповещение об обнаружении индикаторов компрометации. Значение `first` указывает, что извлекаться должно только первое значение, совпавшее с регулярным выражением.
`concatenate`	Задает правило для формирования составного значения из данных, извлеченных из события.
`use_for_retroscan`	Указывает, должно ли извлеченное значение, сопоставленное с указанным регулярным выражением, использоваться для ретроспективного сканирования. Если извлеченное значение должно использоваться для ретроспективного сканирования, для этого атрибута устанавливается значение `true`. Если извлеченное значение не должно использоваться для ретроспективного сканирования, для этого атрибута устанавливается значение `false`.

Значение

Этот элемент содержит регулярное выражение Boost.

Пример

Ниже приведен пример этого элемента.

```
<RE_MD5 type="MD5" extract="all" use_for_retroscan="false">([\da-fA-F]{32})</RE_MD5>
```

ConnectionString

Задает IP-адрес и порт (или именованный канал Windows), который служба будет прослушивать в ожидании входящих событий.

Этот элемент является обязательным.

Путь

`Domains > Domain > InputSettings > ConnectionString`

Атрибуты

У этого элемента есть следующие атрибуты:

Атрибуты элемента «ConnectionString»

Атрибут	Описание
`use_encryption`	Определяет используемое шифрованное соединение.

Значение

Значение имеет формат `<ip_address>:<port>` (если используются IP-адрес и порт) или `\\.\pipe\<pipe_name>` (если используется именованный канал Windows).

> Можно использовать адрес IPv4 или IPv6.

Пример

Ниже приведен пример этого элемента.

```
<ConnectionString use_encryption="TLS">127.0.0.1:9995</ConnectionString>
```

EventDelimiter

Задает правило разделения входящих событий.

Путь

`Domains > Domain > InputSettings` > `EventDelimiter`

Атрибуты

У этого элемента нет атрибутов.

Значение

Правило, задаваемое значением, должно иметь следующий формат:

```
<EventDelimiter>%START_EVENT_SYMBOLS%</EventDelimiter>
```

Значение `%START_EVENT_SYMBOLS%` содержит регулярное выражение, соответствующее началу подстроки входящего события.

Правило обрабатывает все вхождения значения `%START_EVENT_SYMBOLS%`. Если в строке входящего события найдено значение `%START_EVENT_SYMBOLS%`, эта строка разбивается на несколько событий путем добавления символа новой строки (`\n`) перед каждой сопоставленной подстрокой.

Если значение %START_EVENT_SYMBOLS% не совпадает ни с одной подстрокой входящей строки, входящая строка считается единым событием.

> Если событие содержит символы новой строки (\n), разбиение такого события произойдет как по значению %START_EVENT_SYMBOLS%, так и по символу новой строки.

Пример

Ниже приведен пример этого элемента.

```
<EventDelimiter><![CDATA[;]]></EventDelimiter>
```

OutputSettings

Содержит параметры вывода для тенанта.

Задает адрес и порт целевого программного обеспечения, в которое отправляются исходящие оповещения об обнаружении индикаторов компрометации, а также формат исходящих оповещений.

Путь

```
Domains > Domain > OutputSettings
```

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

> Чтобы указать значения элемента *RecordFieldContextFormat*, может потребоваться ознакомление с дополнительной информацией о шаблонах формата оповещений.

Этот элемент является контейнером для следующих вложенных элементов:

- *ConnectionString*

  Задает IP-адрес и порт (или именованный канал Windows), на которые служба будет отправлять исходящие оповещения.

  Этот элемент является обязательным.

  Дополнительные сведения об этом элементе приведены в подразделе «OutputSettings > ConnectionString» ниже.

- *EventSettings*

  Содержит настройки исходящих оповещений, которые отправляет Kaspersky CyberTrace.

- *RecordFieldContextFormat*

  Указывает, как к оповещению должны добавляться поля контекста.

  Этот элемент является обязательным.

- *AlertConnectionString*

  Задает IP-адрес (или хост) и порт, на который служба должна отправлять исходящие оповещения.

  Этот элемент не является обязательным.

  Дополнительные сведения об этом элементе приведены в подразделе «OutputSettings > AlertConnectionString» ниже.

- *AlertFormat*

  Задает формат исходящих оповещений.

  Этот элемент не является обязательным. Если элемент отсутствует в конфигурационном файле, уведомление не формируется.

OutputSettings > ConnectionString

Задает IP-адрес (или хост) и порт, на который служба будет отправлять служебные оповещения.

Строка имеет формат `<ip_address>:<port>` (если используются IP-адрес и порт) или `\\.\pipe\<pipe_name>` (если используется именованный канал Windows).

Можно использовать адрес IPv4 или IPv6.

OutputSettings > AlertConnectionString

Задает IP-адрес (или хост) и порт, на который служба будет отправлять служебные оповещения.

Значение элемента имеет формат `<ip_address>:<port>` (если используются IP-адрес и порт) или `\\.\pipe\<pipe_name>` (если используется именованный канал Windows). IP-адрес должен состоять из четырех десятичных октетов, разделенных точкой. Значение в каждом октете должно быть меньше 256.

Этот элемент не является обязательным. Если элемент пропущен, для этого элемента используется атрибут *enabled* со значением `false`.

У этого элемента есть следующие атрибуты:

Атрибуты элемента «AlertConnectionString»

Атрибут	Описание
`enabled`	Определяет, отправляет ли служба Kaspersky CyberTrace служебные оповещения на указанные IP-адрес и порт. Возможные значения: `true`, `false`. Если значение равно `true`, служба Kaspersky CyberTrace отправляет служебные оповещения на IP-адрес и порт, указанные в этом элементе. Если значение равно `false`, служба Kaspersky CyberTrace отправляет оповещения на IP-адрес и порт, указанные в элементе *OutputSettings → ConnectionString*.
`use_encryption`	Определяет используемое шифрованное соединение.

Пример

Ниже приведен пример этого элемента.

```
<OutputSettings>
     <ConnectionString use_encryption="TLS">127.0.0.1:9995</ConnectionString>
     <EventSettings>
      ...
     </EventSettings>
     <RecordFieldContextFormat><![CDATA[ %ParamName%=%ParamValue%]]></RecordFieldContextFormat>
     <AlertConnectionString enabled="true" use_encryption="TLS">127.0.0.1:9994</AlertConnectionString>
     <AlertFormat>%Date% alert=%Alert%%RecordContext%</AlertFormat>
</OutputSettings>
```

EventSettings

Содержит настройки исходящих оповещений, которые отправляет Kaspersky CyberTrace.

Путь

`Domains > Domain > OutputSettings > EventSettings`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

> Чтобы указать значения элемента *EventFormat* и *ActionableFieldContextFormat*, может потребоваться ознакомление с дополнительной информацией о шаблонах формата оповещений.

Этот элемент является контейнером для следующих вложенных элементов:

- *EventFormat*

  Задает формат исходящих оповещений.

  Этот элемент является обязательным.

- *SendEventFilters*

  Содержит правила фильтрации оповещений об обнаружении индикаторов компрометации из Kaspersky CyberTrace. Можно задать несколько правил фильтрации одновременно.

- *ActionableFieldContextFormat*

  Определяет, каким образом к оповещению должны добавляться поля контекста.

  Этот элемент является обязательным.

- *FinishedEventFormat*

  Задает формат оповещения, создаваемого для каждого обработанного события.

  Этот элемент является обязательным.

  Дополнительные сведения об этом элементе приведены в подразделе «EventSettings > FinishedEventFormat» ниже.

EventSettings > FinishedEventFormat

Задает формат оповещения, которое генерируется после обработки события.

Если этот параметр включен, Kaspersky CyberTrace генерирует оповещение для каждого обрабатываемого события. Оповещение генерируется, даже если обнаружений киберугроз не было.

Этот элемент является обязательным.

Значение этого элемента задает формат оповещения. В формате можно использовать шаблон *%RecordContext%* и имена регулярных выражений.

Если используется шаблон *%RecordContext%*, он предоставляет следующие поля:

- *category*

  Для оповещений данного типа это `LookupFinished`.

- *sent_events*

  Количество оповещений, отправленных в SIEM-систему.

- *total*

  Конкатенация следующих подстрок, сформированных для каждой категории, отнесенной к оповещениям об обнаружении индикаторов компрометации:

  `<category>:<number_of_detections>;`

  Если обнаружений не было, значением параметра *sent_events* является `0`, а значением параметра *total* является пустая строка.

У этого элемента есть следующие атрибуты:

Атрибуты элемента «FinishedEventFormat»

Атрибут	Описание
`enabled`	Определяет, генерируются ли специальные оповещения. Возможные значения: `true`, `false`. Если значение равно `true`, служба Kaspersky CyberTrace генерирует специальные оповещения. Если значение равно `false` или этот атрибут не указан, служба Kaspersky CyberTrace не генерирует специальные оповещения. Этот атрибут не является обязательным.

Пример

Ниже приведен пример этого элемента.

```
<EventSettings>
    <EventFormat>%RE_DATE% category=%Category% matchedIndicator=%MatchedIndicator% url=%RE_URL% src=%SRC_IP%
ip=%RE_IP% md5=%RE_MD5% sha1=%RE_SHA1% sha256=%RE_SHA256% usrName=%RE_USERNAME%%RecordContext%</EventFormat>
    <SendEventFilters>
            ...
    </SendEventFilters>
    <ActionableFieldContextFormat><![CDATA[ %ParamName%:%ParamValue%]]></ActionableFieldContextFormat>
    <FinishedEventFormat enabled="true">LookupFinished %RecordContext%</FinishedEventFormat>
</EventSettings>
```

EventSettings > SendEventFilters

Содержит правила фильтрации оповещений об обнаружении индикаторов компрометации из Kaspersky CyberTrace. Можно задать несколько правил фильтрации одновременно.

Путь

`Domains > Domain > OutputSettings > EventSettings > SendEventFilters`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующего вложенного элемента:

- *Фильтр*

  Правило фильтрации.

SendEventFilters > Filter

Этот элемент задает одно правило фильтрации.

У этого элемента есть следующие атрибуты:

Атрибуты элемента «Filter»

Атрибут	Описание
`attribute`	Имя атрибута индикатора из базы индикаторов, к которому применяются правила фильтрации.
`value`	Правило фильтрации. Kaspersky CyberTrace отправляет оповещение об обнаружении индикаторов компрометации, если значение атрибута индикатора совпадает с указанным.

Пример

Ниже приведен пример этого элемента.

```
<SendEventFilters>
    <Filter attribute="ioc_supplier_context.last_seen" value="[01.02.2013;01.02.2015]"/>
    <Filter attribute="ioc_supplier_context.popularity" value="5"/>
    <Filter attribute="ioc_updated_timestamp" value="[%NOW%-3;%NOW%]"/>
</SendEventFilters>
```

Domain > Feeds > Feed

Определяет конфигурацию для отдельного потока данных об угрозах в рамках тенанта.

Путь

`Domains > Domain > Feeds > Feed`

Атрибуты

У этого элемента есть следующие атрибуты.

Атрибуты элемента «Feed»

Атрибут	Описание
`feedname`	Имя потока данных об угрозах. Должно соответствовать имени потока данных об угрозах в элементе *Feeds > Feed*.
`used`	Указывает, используется ли поток данных в тенанте. Для использования потока данных в тенанте этот поток данных должен быть включен в соответствующем элементе *Feeds > Feed*. Если поток данных включен для тенанта, установлено значение `true`. Если поток данных для тенанта выключен, установлено значение `false`.

Вложенные элементы

Этот элемент является контейнером для следующего вложенного элемента:

- *ActionableFields*

  Задает поля контекста для этого потока данных об угрозах в рамках данного тенанта.

  Этот элемент не является обязательным.

Пример

Ниже приведен пример этого элемента.

```
<Feed feedname="Demo_Botnet_CnC_URL_Data_Feed.json" used="true">
    <ActionableFields>
        ...
    </ActionableFields>
</Feed>
```

ActionableFields

Определяет поля, которые должны вставляться в исходящие оповещения помимо контекста. Исходящее оповещение содержит контекст и поля контекста.

Путь

`Domains > Domain > Feeds > Feed > ActionableFields`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующего вложенного элемента:

- *ActionableField*

  Определяет одно поле контекста.

ActionableFields > ActionableField

Определяет одно поле контекста.

У этого элемента есть следующие атрибуты:

Атрибуты элемента «ActionableField»

Атрибут	Описание
`name`	Имя поля в том виде, в котором оно используется в потоке данных об угрозах
`output_name`	Имя поля в том виде, в котором оно будет вставляться в исходящие оповещения. Если атрибут `output_name` пропущен или содержит пустое значение, имя поля в исходящем событии будет таким же, как имя поля, указанное в потоке данных об угрозах.

Пример

Ниже приведен пример этого элемента.

```
<ActionableFields>
    <ActionableField name="information" output_name="cs4"/>
    <ActionableField name="threat" output_name="cs3"/>
</ActionableFields>
```

IoCExports

Содержит параметры экспорта индикаторов.

Путь

`IoCExports`

Атрибуты

У этого элемента есть следующие атрибуты.

Атрибуты элемента «IoCExports»

Атрибут	Описание
`export_dir`	Путь к каталогу, в котором будет находиться отчет. Этот путь может быть как абсолютным, так и относительным.

Вложенные элементы

Этот элемент является контейнером для следующего вложенного элемента:

- *IoCExport*

  Задает параметры для отдельного отчета с экспортированными данными.

Пример

Ниже приведен пример этого элемента.

```
<IoCExports export_dir="../reports">
                        ...
</IoCExports>
```

IoCExport

Задает настройки для отдельного отчета с экспортированными данными.

Путь

`IoCExports > IoCExport`

Атрибуты

У этого элемента есть следующие атрибуты.

Атрибуты элемента «IoCExport»

Атрибут	Описание
`name`	Имя задачи обновления. Имя может иметь длину от 2 до 64 символов и должно содержать только латинские буквы, цифры (0–9), дефисы (`'-'`) и знаки подчеркивания (`'_'`). Этот атрибут является обязательным.
`enabled`	Указывает, требуется ли формировать отчет. Если отчет должен формироваться, задается значение `true`. Если отчет формироваться не должен, задается значение `false`. Этот атрибут является обязательным.
`delimiter`	Задает правило разделения полей в файле отчета. В качестве разделителя можно использовать один из следующих символов: « `,` », « `;` », « » (символ пробела), « `\t` » (символ табуляции). Этот атрибут является обязательным.
`update_frequency`	Интервал обновления (в минутах) для задачи экспорта. Возможны следующие значения: `0`, `30`, `60`, `120`, `240`, `480`, `960`, `1440`. Этот атрибут является обязательным.

Атрибут	Описание
`create_header`	Указывает, должен ли файл отчета содержать имена столбцов в качестве первой строки. Если файл отчета должен содержать имена столбцов в качестве первой строки, указывается значение `true`. Если файл отчета не должен содержать имена столбцов в качестве первой строки, указывается значение `false`. Этот атрибут является обязательным.
`records_limit`	Максимальное количество показателей, включаемых в отчет. Значение должно быть положительным целым числом. Максимальное количество записей составляет 1 000 000. По умолчанию указано значение 50 000. Этот атрибут является обязательным.
`created_by`	Идентификатор пользователя Kaspersky CyberTrace, создавшего отчет. Этот атрибут является обязательным.
`credentials`	Учетные данные (имя пользователя и пароль), которые должны использоваться в базовой схеме авторизации при запросе отчета. Учетные данные хранятся в зашифрованном виде. Шифрование можно настроить с помощью веб-интерфейса Kaspersky CyberTrace. Это необязательный атрибут.

Вложенные элементы

Этот элемент является контейнером для следующего вложенного элемента:

- *Filter*

  Определяет правила фильтрации экспортируемых данных.

  Конфигурационный файл должен содержать хотя бы один элемент Filter.

Пример

Ниже приведен пример этого элемента.

```
<IoCExport name="report_csv_123" enabled="true" delimiter=";" update_frequency="1440" create_header="true"
records_limit="10000" created_by="admin" credentials="Mhy5QB7R487xbULBQJn8CzpOdV2fQftPyBJPxgjLBXZb+x08">
    ...
</IoCExport>
```

IoCExport > Filter

Определяет правила фильтрации экспортируемых данных.

Путь

`IoCExports > IoCExport > Filter`

Атрибуты

У этого элемента есть следующие атрибуты.

Атрибуты элемента «Filter»

Атрибут	Описание
`field`	Задает имя поля, к которому применяются правила фильтрации и (или) которое необходимо экспортировать. Можно указывать имена атрибутов индикаторов из базы данных индикаторов. Имя может иметь длину от 2 до 255 символов, должно содержать только символы ASCII нижнего регистра и не может начинаться с дефиса («-»), плюса («+») и знака подчеркивания («_»). Не допускаются символ пробела (« ») и символ табуляции. Также в именах атрибутов не допускаются следующие символы: `, | > < " * ? : \ /` Этот атрибут является обязательным.
`value`	Критерии фильтрации для поля. Допустимо использовать любое значение, соответствующее требованиям. Чтобы указать значение, используйте средство выбора дат в календаре. Этот атрибут является обязательным.
`included`	Указывает, необходимо ли включать значения полей в файл отчета. Если значения полей должны включаться в файл отчета, задается значение `true`. Если значения полей не должны включаться в файл отчета, задается значение `false`. Этот атрибут является обязательным.
`output_name`	Задает имя поля, которое должно содержать значения из экспортируемого поля. Этот атрибут является обязательным, если выполняются следующие требования: • Для атрибута `IoCExport > create_header` задано значение `true` • Для атрибута `Filter > included` задано значение `true`
`sort`	Задает порядок сортировки значений полей. Возможны следующие значения: • `asc` Значения сортируются по возрастанию. • `desc` Значения сортируются по убыванию. Этот атрибут не является обязательным.

Пример

Ниже приведен пример этого элемента.

```
<Filter field="ioc_type" value="MD5;SHA1" sort="desc" included="false"/>
<Filter field="supplier_name" value="IP Reputation Data Feed" included="true" output_name="feed"/>
<Filter field="supplier_confidence" value="*" included="false"/>
<Filter field="added_timestamp" value="[*;25.12.2019]" sort="asc" included="false"/>
```

GraphSettings

Задает настройки графа. Этот элемент не является обязательным.

Путь

`GraphSettings`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующих вложенных элементов:

- *KLTipToken*

  Токен доступа, который Kaspersky CyberTrace использует для подключения к Kaspersky Threat Intelligence Portal. Этот параметр хранится в зашифрованном виде. Этот параметр можно изменить в веб-интерфейсе Kaspersky CyberTrace.

  Этот элемент не является обязательным.

Пример

Ниже приведен пример этого элемента.

```
<GraphSettings>
    <KLTipToken>I6gHGp8JK3o0nJ+NkUg2oA==</KLTipToken>
</GraphSettings>
```

Plugins

Содержит настройки плагинов Kaspersky CyberTrace.

Путь

`Plugins`

Атрибуты

У этого элемента нет атрибутов.

Вложенные элементы

Этот элемент является контейнером для следующего вложенного элемента:

- *Plugin*

  Описывает отдельный плагин Kaspersky CyberTrace.

Пример

Ниже приведен пример этого раздела.

```
<Plugins>
    ...
</Plugins>
```

Plugin

Описывает отдельный плагин Kaspersky CyberTrace.

Путь

```
Plugins > Plugin
```

Атрибуты

У этого элемента есть следующий атрибут:

Атрибут	Описание
`Plugin id`	Задает значение идентификатора плагина.

Вложенные элементы

Наличие вложенных элементов зависит от конкретного плагина.

Пример

Ниже приведен пример этого элемента.

```
<Plugin id="kl_graph_virustotal_enrichment">
    <APIBaseURL>https://www.virustotal.com/api/v3</APIBaseURL>
    <APIToken>VmVyeSBzdHJvbmcgcGFzc3dvcmQ=</APIToken>
</Plugin>
```

Включение инкрементных потоков данных об угрозах

Kaspersky CyberTrace поддерживает использование инкрементных версий потоков данных об угрозах Kaspersky Threat Data Feeds. Дополнительные сведения о инкрементных потоках данных об угрозах и о способах их загрузки приведены в подразделе «Загрузка инкрементных потоков данных об угрозах» раздела Работа с потоками данных об угрозах.

Инкрементные версии похожи на обыкновенные потоки данных об угрозах, но имеют другие идентификаторы. Эти идентификаторы хранятся в дополнительных конфигурационных файлах, входящих в состав комплекта поставки, и располагаются в следующих каталогах:

Расположение дополнительных конфигурационных файлов

Конфигурационный файл	Расположение (Linux)	Расположение (Windows)
`kl_feed_util_diff.conf`	`etc/`	`bin\`
`kl_feed_info_diff.conf`	`httpsrv/etc/`	`httpsrv\etc\`

Чтобы включить загрузку инкрементных потоков данных об угрозах после установки, сразу же после установки Kaspersky CyberTrace выполните следующие действия:

1. Остановите Kaspersky CyberTrace Service.
2. Переименуйте файл `kl_feed_util.conf` (например, в `kl_feed_util.conf.0`).
3. Переименуйте файл `kl_feed_info.conf` (например, в `kl_feed_info.conf.0`).
4. Переименуйте файл `kl_feed_util_diff.conf` в `kl_feed_util.conf`.
5. Укажите `accepted` в разделе `Settings > EULA` файла `kl_feed_util.conf`.
6. Переименуйте `kl_feed_info_diff.conf` в `kl_feed_info.conf`.
7. Запустите Kaspersky CyberTrace Service.
8. Выполните первоначальную настройку.

Чтобы включить загрузку инкрементных потоков данных об угрозах после обновления, сразу же после обновления Kaspersky CyberTrace выполните следующие действия:

1. Остановите Kaspersky CyberTrace Service.
2. Создайте копию файла `kl_feed_util.conf`, затем переименуйте эту копию (например, в `kl_feed_util.conf.0`).
3. В элементе `Settings > Feeds > Feed` файла `kl_feed_util.conf` измените старые идентификаторы потоков данных об угрозах на новые в соответствии с таблицей ниже.
4. Создайте копию файла `kl_feed_info.conf`, затем переименуйте эту копию (например, в `kl_feed_info.conf.0`).
5. В файле `kl_feed_info.conf` измените старые идентификаторы потоков данных об угрозах на новые в соответствии с таблицей ниже.
6. Запустите Kaspersky CyberTrace Service.

Идентификаторы потоков данных об угрозах

Поток данных об угрозах	Старый идентификатор (без инкрементной части)	Новый идентификатор
Botnet C&C URL	65	152
Phishing URL	59	153
Malicious URL	64	154

Журнал Kaspersky CyberTrace Service

В этом разделе описывается порядок ведения журнала работы Kaspersky CyberTrace Service.

Включение ведения журнала

По умолчанию ведение журнала отключено. Включить ведение журнала можно в файле kl_feed_service_log.conf в каталоге `bin`, где расположен бинарный файл службы. Заполните файл kl_feed_service_log.conf, как описано в этом разделе. Изменение содержимого файла kl_feed_service_log.conf приводит к применению новых настроек, этот процесс занимает несколько секунд.

Включение ведения журнала снижает производительность Kaspersky CyberTrace Service. Ведение журнала следует включать только в случае возникновения проблем и ошибок.

Ведение журнала также можно включить и настроить в веб-интерфейсе Kaspersky CyberTrace.

Ведение журнала и безопасность данных

Если ведение журнала включено, Kaspersky CyberTrace Service может записывать в файлы журнала любые из следующих сведений, которые можно считать конфиденциальными:

- Исходные события (URL, IP-адреса, хеши и другие данные) в том виде, в каком они поступили в Kaspersky CyberTrace Service.
- Результаты сопоставления исходных событий с потоками данных об угрозах.

Файлы журнала представляют собой простые текстовые файлы. Вся информация записывается в файлы журнала в незашифрованном виде. Файлы журнала имеют стандартные унаследованные права доступа. Рекомендуется назначить каталогу для хранения файлов журнала соответствующие права, чтобы читать файлы журнала мог только администратор.

Kaspersky CyberTrace не отправляет файлы журналов или какие-либо данные, содержащиеся в них, в «Лабораторию Касперского». В целях оказания технической поддержки ваш менеджер по работе с клиентами может попросить вас предоставить файлы журнала.

Файлы журнала хранятся до тех пор, пока они не будут явным образом удалены пользователем. Если параметр `Append` в конфигурационном файле ведения журналов имеет значение `0`, старые файлы журнала удаляются при запуске Kaspersky CyberTrace Service. Если параметр `Append` в конфигурационном файле ведения журнала имеет значение `1`, информация сохраняется в течение всего цикла использования Kaspersky CyberTrace Service.

В случае удаления Kaspersky CyberTrace эти файлы журналов не удаляются, если каталог с файлами журналов находится за пределами каталога установки Kaspersky CyberTrace Service (в соответствии со значением параметра `LogsFolder`).

Дополнительную информацию о данных, записываемых в файлы журнала, см. ниже в подразделе «Содержимое файла журнала».

Конфигурационный файл журнала

Файл kl_feed_service_log.conf представляет собой файл XML. Его поля описаны в таблице ниже.

Параметр	Описание	Обязательный/необязательный
WriteLog	Уровень ведения журналов. Можно использовать одно из следующих значений: • `non` — ведение журналов выключено. • `err` — регистрируются только ошибки. • `inf` — регистрируются ошибки и информационные сообщения. • `dbg` — регистрируются все сообщения. • `any` — регистрируются все сообщения, включая служебную информацию.	Необязательный По умолчанию задано значение `non`.
LogsFolder	Каталог, в котором хранятся файлы журнала. Могут использоваться абсолютные и относительные пути. В Windows в параметре `LogsFolder` не допускаются следующие символы: `?`, `*`, `#`, `$`, `:`, `"`, `<`, `>`, `|`. Если в параметре `LogsFolder` используются переменные среды, они не будут развернуты, а будут использоваться как есть.	Необязательный По умолчанию подкаталог `logs` каталога, в котором находится исполняемый файл службы.
SizeLimit	Максимальный размер файла журнала в МБ. Если задано значение `0`, размер файла журнала не ограничен.	Необязательный По умолчанию задано значение `0`.
Append	Указывает, следует ли удалять старые файлы журнала (`false`) или добавить новые записи в существующий файл (`true`). Если указано пустое значение, это означает, что данные в журнал не записываются вовсе (эквивалентно указанию `<WriteLog>non</WriteLog>`).	Необязательный По умолчанию задано значение `false`.
UseSyslog	Указывает, будет ли для ведения журнала использоваться системный демон syslog (`true`) или нет (`false`). В Windows этот параметр не используется.	Необязательный По умолчанию задано значение `true`.

Пример конфигурационного файла

В следующем примере файла kl_feed_service_log.conf включается ведение журнала на уровне ведения журнала `dbg`. Журналы будут храниться в подкаталоге `logs` того каталога, в котором находится двоичный файл Kaspersky CyberTrace Service.

```
<Logging>
        <WriteLog>dbg</WriteLog>
        <LogsFolder>logs</LogsFolder>
        <SizeLimit>0</SizeLimit>
        <Append>false</Append>
        <UseSyslog>true</UseSyslog>
</Logging>
```

Формат имен файлов журналов

Kaspersky CyberTrace Service записывает сообщения в файлы с именами «`kl_feed_service-<pid>-<date_time>.log`» или «`kl_feed_service-<pid>-<date_time>_<index>.log`».

Содержимое файла журнала

Если используется уровень ведения журнала `err`, Kaspersky CyberTrace Service записывает в журнал информацию об ошибках, возникающих в продукте. Этот уровень в файле журнала маркируется как ERR.

Если используется уровень ведения журнала `inf`, Kaspersky CyberTrace Service записывает в журнал важные оповещения о том, что происходит в продукте. Этот уровень в файле журнала маркируется как INF.

Если используется уровень ведения журнала `dbg`, Kaspersky CyberTrace Service записывает в журнал подробную отладочную информацию о том, что происходит в продукте. Этот уровень в файле журнала маркируется как DBG.

Если используется уровень ведения журнала `warn`, Kaspersky CyberTrace Service записывает в журнал информацию о предупреждениях в продукте. Этот уровень в файле журнала маркируется как WARN.

О повторной отправке оповещений об обнаружении индикаторов компрометации

По умолчанию, если во время отправки оповещения об обнаружении индикаторов компрометации в SIEM-систему возникает ошибка, это оповещение повторно по истечении времени, указанного в конфигурационном файле.

Число попыток отправки каждого оповещения об обнаружении индикаторов компрометации и интервал между попытками можно настроить в элементах `EventSendingRetriesCount` и `EventSendingRetriesTimeout` конфигурационного файла.

Kaspersky CyberTrace Service в режиме ReplyBack mode

В некоторых случаях службе Kaspersky CyberTrace необходимо отправлять ответные оповещения в источник событий в тот же сокет, из которого получены исходные события (*режим ReplyBack*).

Чтобы переключить Kaspersky CyberTrace Service в режим ReplyBack, выполните следующие действия:

Отправьте `X-KF-ReplyBack` в качестве первого сообщения после установления TCP-соединения с Kaspersky CyberTrace Service.

На протяжении текущей сессии TCP каждое ответное оповещение будет отправляться обратно в тот же сокет, из которого было получено исходное событие. Настройка, указанная в элементе `OutputSettings > ConnectionString` конфигурационного файла, будет проигнорирована.

Для службы Kaspersky CyberTrace можно настроить отправку оповещения, свидетельствующего о том, что проверка события завершена.

Чтобы включить отправку оповещений о завершении, выполните одно из следующих действий:

- Установите для атрибута `enable` элемента `OutputSettings > EventSettings > FinishedEventFormat` конфигурационного файла Kaspersky CyberTrace Service значение `true`.
- Отправьте `X-KF-SendFinishedEventX-KF-ReplyBack` в качестве первого сообщения после установления TCP-соединения с Kaspersky CyberTrace Service.

  В этом случае атрибут `enable` элемента `EventSettings > FinishedEventFormat` в конфигурационном файле Kaspersky CyberTrace Service будет проигнорирован.

Чтобы дать службе Kaspersky CyberTrace указание перейти в режим ReplyBack и отправлять оповещения о завершении, выполните следующие действия:

Отправьте `X-KF-SendFinishedEventX-KF-ReplyBack` в качестве первого сообщения после установления TCP-соединения с Kaspersky CyberTrace Service.

По умолчанию в режиме ReplyBack Kaspersky CyberTrace не сохраняет статистику оповещений об обнаружении индикаторов компрометации, полученных во время текущей сессии соединения.

Чтобы сохранять статистику оповещений об обнаружении индикаторов компрометации в режиме ReplyBack, выполните следующие действия:

- Если служба Kaspersky CyberTrace должна отправлять оповещения о завершении, отправьте `X-KF-SendFinishedEventX-KF-ReplyBackX-KF-SaveStatistic` в качестве первого сообщения после установления TCP-соединения со службой Kaspersky CyberTrace.
- Если служба Kaspersky CyberTrace не должна отправлять оповещения о завершении, отправьте `X-KF-ReplyBackX-KF-SaveStatistic` в качестве первого сообщения после установления TCP-соединения со службой Kaspersky CyberTrace.

Особенности обработки событий в Kaspersky CyberTrace Service

В этом разделе описывается обработка входящих событий в Kaspersky CyberTrace Service.

Kaspersky CyberTrace Service получает и отправляет события по протоколу TCP. Для событий используется кодировка UTF-8.

Kaspersky CyberTrace Service обрабатывает специальные символы во входящих событиях следующим образом:

- Kaspersky CyberTrace Service рассматривает символ перевода строки (0x0A) как разделитель между событиями.

  Таким образом, текст перед символом перевода строки и текст после него относятся к разным событиям.
- Kaspersky CyberTrace Service игнорирует символ возврата каретки (0x0D).

Ограничения на входящие события Kaspersky CyberTrace Service

Kaspersky CyberTrace Service обрабатывает события размером не более 64 килобайт (КБ). Если входящее событие превышает 64 КБ, Kaspersky CyberTrace Service разбивает его на несколько событий и обрабатывает их отдельно. Таким образом, индикатор может оказаться разделенным на две части и в результате он не будет извлечен и проверен.

Рекомендуется настроить источник событий (программное обеспечение SIEM), или правила нормализации, или и то и другое таким образом, чтобы размер входящих событий не превышал 64 КБ.

Расширение категорий обнаруженных киберугроз

Начиная с версии Kaspersky CyberTrace 4.0, обнаружение по некоторым полям потоков данных было отключено, соответственно, были отключены и соответствующие категории обнаружений киберугроз (см. список ниже).

- Botnet C&C URL Data Feed и Demo Botnet C&C URL Data Feed:
  - KL_BotnetCnC_Hash_MD5
  - KL_BotnetCnC_Hash_SHA1
  - KL_BotnetCnC_Hash_SHA256
- IP Reputation Data Feed и Demo IP Reputation Data Feed:
  - KL_IP_Reputation_Hash_MD5
  - KL_IP_Reputation_Hash_SHA1
  - KL_IP_Reputation_Hash_SHA256
- Malicious URL Data Feed:
  - KL_Malicious_URL_Hash_MD5
  - KL_Malicious_URL_Hash_SHA1
  - KL_Malicious_URL_Hash_SHA256
- Mobile Botnet C&C URL Data Feed:
  - KL_Mobile_BotnetCnC_Hash_MD5
  - KL_Mobile_BotnetCnC_Hash_SHA1
  - KL_Mobile_BotnetCnC_Hash_SHA256

- Ransomware URL Data Feed:
  - KL_Ransomware_URL_Hash_MD5
  - KL_Ransomware_URL_Hash_SHA1
  - KL_Ransomware_URL_Hash_SHA256

Чтобы включить обнаружение событий для этих категорий, выполните следующие действия:

1. Остановите Kaspersky CyberTrace Service.

   `systemctl stop cybertrace.service` (в Linux)

   `sc stop cybertrace` (в Windows)

2. Откройте конфигурационный файл:
   - Windows: `httpsrv\etc\kl_feed_info.conf`
   - Linux: `httpsrv/etc/kl_feed_info.conf`

3. Добавьте необходимые категории в элемент `fields` потока данных об угрозах. Подробная информация о категориях, которые можно добавить, приведена в таблице ниже.

   Например, чтобы включить обнаружение по MD5, SHA1 и SHA256 для потока данных об угрозах Botnet C&C URL Data Feed, отредактируйте файл `kl_feed_info.conf` следующим образом:

```
{
        "name": "Botnet_CnC_URL_Data_Feed",
        "id": 65,
        "description": "A set of URLs and hashes with context that cover desktop botnet C&amp;C servers and
related malicious objects. Masked and non-masked records are available.",
        "fields": [
            { "name": "mask", "type": "URL", "category": "KL_BotnetCnC_URL" },
            { "name": "files/MD5", "type": "MD5", "category": "KL_BotnetCnC_Hash_MD5" },
             { "name": "files/SHA1", "type": "SHA1", "category": "KL_BotnetCnC_Hash_SHA1" },
             { "name": "files/SHA256", "type": "SHA256", "category": "KL_BotnetCnC_Hash_SHA256" } ],
        "verification": [
            { "indicator": "http://fakess123bn.nu/", "category": "KL_BotnetCnC_URL" } ]
 }
```

4. Запустите Kaspersky CyberTrace Service.

   `systemctl start cybertrace.service` (в Linux)

   `sc start cybertrace` (в Windows)

5. Откройте веб-интерфейс Kaspersky CyberTrace. Перейдите в раздел **Параметры** → **Потоки данных**, затем запустите обновление потоков данных об угрозах кнопкой (**Обновить сейчас**).

В таблице ниже приведены значения для элементов `name`, `type` и `category` в файле `kl_feed_info.conf`.

Категории, которые можно добавить в потоки данных об угрозах

Имя	Тип	Категория
Botnet C&C URL Data Feed и Demo Botnet C&C URL Data Feed		
files/MD5	MD5	KL_BotnetCnC_Hash_MD5
files/SHA1	SHA1	KL_BotnetCnC_Hash_SHA1
files/SHA256	SHA256	KL_BotnetCnC_Hash_SHA256
IP Reputation Data Feed и Demo IP Reputation Data Feed		

Имя	Тип	Категория
files/MD5	MD5	KL_IP_Reputation_Hash_MD5
files/SHA1	SHA1	KL_IP_Reputation_Hash_SHA1
files/SHA256	SHA256	KL_IP_Reputation_Hash_SHA256
Malicious URL Data Feed		
files/MD5	MD5	KL_Malicious_URL_Hash_MD5
files/SHA1	SHA1	KL_Malicious_URL_Hash_SHA1
files/SHA256	SHA256	KL_Malicious_URL_Hash_SHA256
Mobile Botnet C&C URL Data Feed		
files/MD5	MD5	KL_Mobile_BotnetCnC_Hash_MD5
files/SHA1	SHA1	KL_Mobile_BotnetCnC_Hash_SHA1
files/SHA256	SHA256	KL_Mobile_BotnetCnC_Hash_SHA256
Ransomware URL Data Feed		
files/MD5	MD5	KL_Ransomware_URL_Hash_MD5
files/SHA1	SHA1	KL_Ransomware_URL_Hash_SHA1
files/SHA256	SHA256	KL_Ransomware_URL_Hash_SHA256

После выполнения действий, описанных в этом разделе, Kaspersky CyberTrace выполняет следующие действия: в дополнение к загрузке IP-адресов и масок при загрузке в базу индикаторов потоков данных об угрозах «Лаборатории Касперского» Kaspersky CyberTrace также загружает индикаторы, соответствующие хешам. В результате для потоков данных об угрозах, перечисленных в этом разделе, Kaspersky CyberTrace обнаруживает события не только по IP-адресам и маскам, но и по хешам файлов.

Руководство по Feed Utility

В этом разделе описывается порядок работы с Feed Utility.

Работа с потоками данных об угрозах

Feed Utility представляет собой инструмент, позволяющий загружать, фильтровать и компилировать потоки данных об угрозах Kaspersky Threat Data Feeds в соответствии с заданным набором правил, определенным в соответствующем конфигурационном файле. Эти правила также можно задавать с помощью веб-интерфейса Kaspersky CyberTrace.

Загрузка данных с серверов

Feed Utility загружает архивы, содержащие потоки данных об угрозах, с серверов обновлений «Лаборатории Касперского». Каждый загруженный архив содержит один поток данных об угрозах. Прежде чем загрузить потоки данных об угрозах Kaspersky Threat Data Feeds, Feed Utility проверяет, новее ли они, чем используемые. Перед загрузкой потоков данных об угрозах OSINT и сторонних потоков данных об угрозах Feed Utility такую проверку не выполняет.

Для аутентификации Feed Utility использует сертификат. Этот сертификат также определяет, какие потоки данных об угрозах Kaspersky Threat Data Feeds могут загружаться с помощью Feed Utility. Например, если используется демо-сертификат для доступа к потокам данных об угрозах от «Лаборатории Касперского», Feed Utility может загружать только демонстрационные потоки данных об угрозах.

В случае проблем с загрузкой потоков данных об угрозах из сторонних источников, обратитесь к разделу Устранение неполадок Feed Utility, подразделу «Ошибка SSL при загрузке стороннего потока данных об угрозах».

Если «Лаборатория Касперского» выпускает новый поток данных об угрозах, и этот поток доступен с вашим сертификатом, добавьте новый элемент `Feed` в конфигурационный файл Feed Utility:

```
<Feed enabled="true">
    <Name>Имя нового потока данных об угрозах</Name>
    <FeedID>Идентификатор нового потока данных об угрозах</FeedID>
</Feed>
```

После добавления нового элемента `Feed` Feed Utility сможет обрабатывать новый поток данных об угрозах.

Чтобы получить список потоков данных об угрозах, доступных с вашим сертификатом, укажите параметр `-l` или `--list` при запуске Feed Utility в командной строке.

Загрузка инкрементных потоков данных об угрозах

Feed Utility поддерживает загрузку инкрементных обновлений для отдельных потоков данных об угрозах Kaspersky Threat Data Feeds. В этом документе такие потоки данных об угрозах называются инкрементными потоками данных об угрозах. Инкрементные потоки данных об угрозах похожи на обычные потоки данных об угрозах Kaspersky Threat Data Feeds, обновляются по обычному сценарию, но имеют другие идентификаторы потоков. См. также список доступных инкрементных потоков данных об угрозах.

Чтобы скачать инкрементный поток данных об угрозах, выполните следующие действия:

Укажите идентификатор инкрементного потока данных об угрозах в конфигурационном файле Feed Utility.

Для них на серверах обновлений «Лаборатории Касперского» формируются срез данных (полная версия потока данных об угрозах) и инкрементная часть (изменения, применение которых к потоку данных об угрозах приводит его в актуальное состояние). Срез данных генерируется ежедневно, инкрементная часть – в соответствии с частотой обновления потока. Инкрементная часть содержит изменения, применение которых к потоку данных об угрозах приводит его в актуальное состояние.

Feed Utility обновляет инкрементные потоки данных об угрозах следующим образом:

1. Срез данных загружается в следующих случаях:

   - Поток данных об угрозах загружается впервые.
   - Поток данных об угрозах в последний раз обновлялся слишком давно и загрузить инкрементные части не представляется возможным.

     Возможность загрузки инкрементных частей определяется на стороне сервера обновлений.

2. Один или несколько архивов с инкрементными частями загружаются, если они новее, чем срез данных, загруженный на шаге 1, или если файл потока данных об угрозах в настоящее время используется.

   При загрузке архива с инкрементной частью он переименовывается в `%FILE_NAME_SRC%_%TIMESTAMP%.zip`, где `%FILE_NAME_SRC%` — первоначальное имя файла (без расширения), а `%TIMESTAMP%` — метка времени момента опубликования инкрементной части в формате `yyyy-mm-dd HH:MM:SS`.

3. Если Feed Utility работает в режиме обработки (с параметром `-p`), ранее загруженные и распакованные инкрементные части применяются к срезу данных, расположенному в каталоге `WorkDir` (подробнее о параметре `WorkDir` в конфигурационном файле Feed Utility).

   При распаковке архива с инкрементной частью она переименовывается в `%FILE_NAME_SRC%_%TIMESTAMP%.json`, где `%FILE_NAME_SRC%` — первоначальное имя файла (без расширения), а `%TIMESTAMP%` — метка времени момента опубликования инкрементной части в формате `yyyy-mm-dd HH:MM:SS`.

По умолчанию Feed Utility загружает инкрементные части потока данных об угрозах параллельно. Чтобы включить последовательную загрузку, задайте для параметра `SequentialDownload` в конфигурационном файле Feed Utility значение `True`.

Инкрементные версии потока данных об угрозах Kaspersky Threat Data Feeds (если они существуют) можно загрузить с помощью того же сертификата, что используется для обычных версий.

Обработка и фильтрация

После загрузки архивов, содержащих потоки данных об угрозах, Feed Utility распаковывает архивы и обрабатывает исходные файлы потоков данных об угрозах. Файлы потоков данных об угрозах изменяются в соответствии с комбинацией правил потоков данных об угрозах, правил фильтрации и других параметров, указанных в конфигурационном файле Feed Utility. Эти параметры определяют данные, которые будут включаться в полученные потоки данных об угрозах, формат вывода полученных потоков данных об угрозах и максимальное количество записей в полученном потоке данных об угрозах.

Фильтрация заключается в изменении исходных файлов потоков данных об угрозах в соответствии с заданными критериями фильтрации. Критерии фильтрации определяются в правилах фильтрации для каждого потока данных об угрозах. В зависимости от предполагаемого сценария использования Feed Utility можно создать поток данных об угрозах, использующий только часть информации, содержащейся в исходном потоке данных об угрозах. Этого можно добиться с помощью комбинации правил потока данных об угрозах и правил фильтрации.

Правила фильтрации по умолчанию

Конфигурационный файл приложения Feed Utility по умолчанию, входящий в состав комплекта поставки Kaspersky CyberTrace, содержит следующее правило фильтрации для потоков данных об угрозах IP Reputation Data Feed и Demo IP Reputation Data Feed:

Загружаются только те записи потока данных об угрозах, у которых значение параметра `threat_score` не менее `75`.

Kaspersky считает вредоносными IP-адреса, у которых значение `threat_score` не ниже `75`. IP-адреса, у которых значение `threat_score` меньше `75`, считаются связанными со спамом и не представляющими существенной угрозы.

Если уменьшить пороговое значение или удалить фильтр, это приведет к большому количеству сообщений об обнаруженных киберугрозах с помощью потоков данных об угрозах Demo IP Reputation Data Feed и IP Reputation Data Feed. Данные сообщения будут уведомлениями об обнаружении IP-адресов, с которых производится рассылка спама.

Чтобы удалить фильтр, выполните следующие действия:

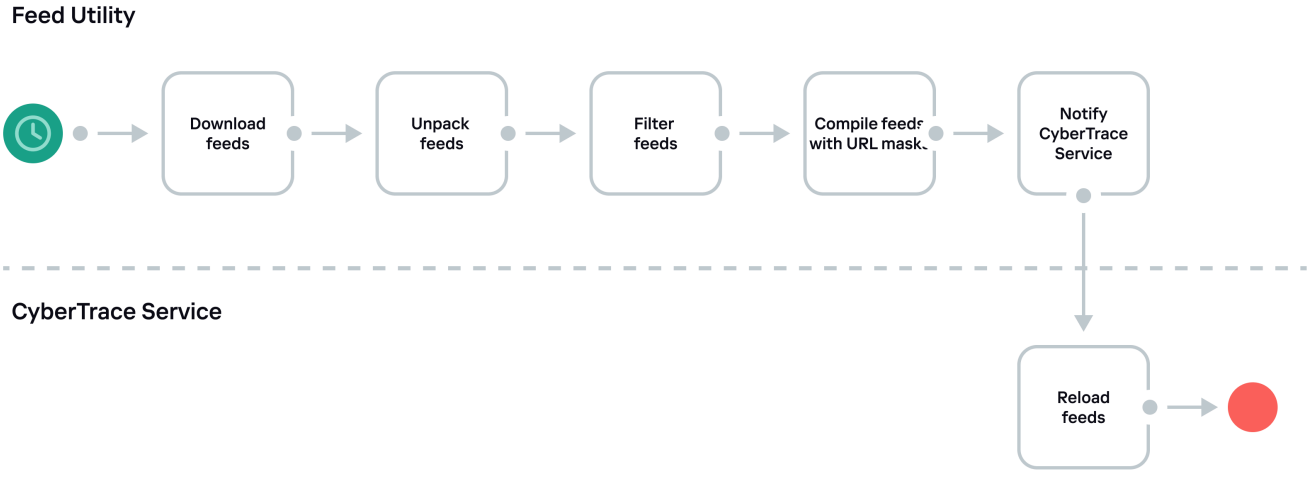
1. Откройте страницу **Параметры → Потоки данных** в веб-интерфейсе Kaspersky CyberTrace.
2. В случае потока данных об угрозах Demo IP Reputation Data Feed (или IP Reputation Data Feed) удалите правило фильтрации по полю `threat_score`.

Компиляция

Если Feed Utility используется совместно с Kaspersky CyberTrace Service, потоки данных об угрозах, содержащие маски URL, должны быть преобразованы в двоичный формат. Feed Utility компилирует маски URL, извлеченные из этих потоков данных об угрозах, и создает двоичные файлы, которые затем используются в Kaspersky CyberTrace Service для быстрого сопоставления URL из полученных событий с масками URL. Feed Utility производит компиляцию автоматически, если в правилах потоков данных об угрозах указан параметр `UrlMatcherField`.

Перезагрузка

При получении соответствующего уведомления Kaspersky CyberTrace Service перезагружает потоки данных об угрозах, которые требуется использовать. Это значит, что старые потока данных об угрозах выгружаются из памяти, а новые загружаются в память.



Обновление потоков данных об угрозах

Параметры командной строки Feed Utility

Feed Utility представляет собой консольное приложение. Его можно вызвать его из командной строки.

Синтаксис

В ОС Linux Feed Utility использует следующий синтаксис:

```
./kl_feed_util [options]
```

В ОС Windows Feed Utility использует следующий синтаксис:

```
kl_feed_util.exe [options]
```

Параметры

Доступны следующие параметры:

- `-h [ --help ]`

  Вывод справочного сообщения.

- `-v [ --verbose ]`

  Включение подробного режима.

  Если включен подробный режим, Feed Utility выводит на экран подробную информацию о выполняемых действиях. Если подробный режим выключен, выводится краткая информация.

- `-s [ --silent ]`

  Включение режима подавления вывода.

  Если включен режим подавления вывода, Feed Utility не выводит на экран информацию о выполняемых действиях.

- `-c [ --config ] arg`

  Задает путь к конфигурационному файлу Путь указывается в аргументе `arg`.

  Можно использовать как абсолютные, так и относительные пути. Если указан относительный путь, он отсчитывается относительно бинарного файла Feed Utility.

  Значение по умолчанию для этого параметра — `kl_feed_util.conf`. Feed Utility ищет этот файл в каталоге, в котором находится бинарный файл Feed Utility.

- `-d [ --download ]`

  Включение режима загрузки.

  Если указан этот параметр, Feed Utility загружает потоки данных об угрозах, но не обрабатывает их.

  Загруженные файлы располагаются в каталоге, указанном в параметре `WorkDir` конфигурационного файла Feed Utility.

- `-u [ --unpack ]`

  Распаковка загруженных потоков данных об угрозах.

  Если указан этот параметр, Feed Utility распаковывает потоки данных об угрозах после загрузки.

  Этот параметр можно использовать только в сочетании с параметром `-d` или `-p`.

- `-p [ --processing ]`

  Включение режима обработки.

  Если указан этот параметр, Feed Utility обрабатывает потоки данных об угрозах, но не загружает и не распаковывает их. Feed Utility не удаляет исходные файлы потоков данных об угрозах.

  Feed Utility ищет потоки данных об угрозах в каталоге, указанном в параметре `WorkDir` конфигурационного файла Feed Utility.

  > В режиме обработки Feed Utility не удаляет исходные файлы потоков данных об угрозах, расположенные в каталоге `WorkDir`. В результате в этом каталоге может оказаться несколько версий одного файла потока данных об угрозах. В этом случае Feed Utility выводит в консоль сообщение об ошибке. Чтобы избежать этой ситуации, необходимо вручную удалить исходные файлы потоков данных об угрозах из каталога `WorkDir` после их обработки Feed Utility.

- `-f [--feed] arg`

  Загрузка или обработка указанного потока данных об угрозах.

  Имя потока данных об угрозах указывается в аргументе `arg`. Это имя должно соответствовать значению параметра `Name`, указанному в правилах потока данных об угрозах (`Feeds` > `Feed` > `Name`).

  Можно указать несколько потоков данных об угрозах. В этом случае названия потоков данных об угрозах разделяются точкой с запятой («`;`»).

  Этот параметр можно использовать с параметрами `-d` и `-p`.

- `-i [--input]`

  Парсинг внешнего потока данных об угрозах с преобразованием его в формат JSON в соответствии с правилами парсинга, определенными для этого потока данных об угрозах.

  Имя потока данных об угрозах указывается в формате `-f`.

- `-l [ --list ]`

  Выводит в консоль список потоков данных об угрозах, доступных с текущим сертификатом и информацию о том, указан ли каждый из потоков данных об угрозах в конфигурационном файле Feed Utility: строка `used` в выводе означает, что поток данных об угрозах указан в конфигурационном файле, а строка `unused` означает, что этот поток данных об угрозах там не указан. Поток данных об угрозах указанный в конфигурационном файле (`used`), может быть как включенным, так и отключенным.

  Этот параметр можно использовать в сочетании с параметром `-c` или `-v`.

- `--set-proxy username:password@host:port`

  Записывает указанные параметры соединения с прокси в конфигурационный файл Feed Utility. Параметры `username` и `password` записываются в зашифрованном виде.

  Имя пользователя указывается в параметре `username`, пароль — в параметре `password`, а адрес и порт прокси-сервера — в параметрах `host` и `port`.

  Если прокси-сервер не требует аутентификации, следует использовать формат `--set-proxy host:port`.

- `--set-taxii username:password@feedname@taxii-address@collectionname`

Записывает указанные параметры соединения с сервером TAXII в конфигурационный файл Feed Utility. Параметры `username` и `password` записываются в зашифрованном виде.

Если сервер TAXII не требует аутентификации, следует использовать формат `feedname@taxii-address@collectionname`.

- `--set-basic-auth username:password@feedname`

  Записывает указанные базовые настройки аутентификации в конфигурационный файл Feed Utility. Параметры `username` и `password` записываются в зашифрованном виде.

  Если пароль не требуется, следует использовать формат `username:@feedname`.

- `--speedtest`

  Измерение средней скорости, с которой Feed Utility загружает потоки данных об угрозах с серверов «Лаборатории Касперского».

  Этот параметр можно комбинировать с параметром `-c` и указать путь к конфигурационному файлу, который требуется использовать.

- `--set-mailbox`

  Для подключения к почтовому серверу Feed Utility кодирует имя пользователя и пароль с помощью этого параметра.

  В параметре `--set-mailbox` указывается атрибут `{user}:{pass}@{FeedName}`,

  где:

  `{user}` — учетная запись пользователя для подключения к почтовому серверу.

  `{pass}` — пароль учетной записи пользователя для подключения к почтовому серверу.

  `{FeedName}` – имя потока данных об угрозах, для которого настраивается подключение.

  > Если в имени потока данных об угрозах есть пробел, такое имя следует заключать в кавычки.

- `--check-mailbox-connection`

  Для проверки соединения с почтовым сервером в параметре `--check-mailbox-connection` следует указать атрибут `{FeedName}`, где `{FeedName}` — имя потока данных об угрозах, для которого требуется проверить параметры подключения.

  > Если в имени потока данных об угрозах есть пробел, такое имя следует заключать в кавычки.

Примеры синтаксиса

Запуск Feed Utility с параметрами по умолчанию. Feed Utility загрузит, распакует и обработает потоки данных об угрозах.

- В ОС Linux:

  ```
  ./kl_feed_util
  ```

- В ОС Windows:

  ```
  kl_feed_util.exe
  ```

Запуск Feed Utility в подробном режиме с конфигурационным файлом `custom_configuration.conf`, расположенным в том же каталоге, что и бинарный файл Feed Utility.

- В ОС Linux:
  ```
  ./kl_feed_util -v -c custom_configuration.conf
  ```
- В ОС Windows:
  ```
  kl_feed_util.exe -v -c custom_configuration.conf
  ```

Загрузка и распаковка потоков данных об угрозах.

- В ОС Linux:
  ```
  ./kl_feed_util -d -u
  ```
- В ОС Windows:
  ```
  kl_feed_util.exe -d -u
  ```

Обработка распакованных потоков данных об угрозах. В этом случае Feed Utility не загружает потоки данных об угрозах, а только ищет распакованные файлы потоков данных об угрозах и обрабатывает их.

- В ОС Linux:
  ```
  ./kl_feed_util -p
  ```
- В ОС Windows:
  ```
  kl_feed_util.exe -p
  ```

Распаковка и обработка потоков данных об угрозах.

- В ОС Linux:
  ```
  ./kl_feed_util -u -p
  ```
- В ОС Windows:
  ```
  kl_feed_util.exe -u -p
  ```

Загрузка, распаковка и обработка указанного потока данных об угрозах.

- В ОС Linux:
  ```
  ./kl_feed_util -f Demo_Botnet_CnC_URL_Data_Feed
  ```
- В ОС Windows:
  ```
  kl_feed_util.exe -f Demo_Botnet_CnC_URL_Data_Feed
  ```

Указание параметров подключения к прокси-серверу. Эти параметры записываются в конфигурационный файл.

- В ОС Linux:
  ```
  ./kl_feed_util --set-proxy 'user:pass@proxy.example.com:3128'
  ```
- В ОС Windows:
  ```
  kl_feed_util.exe --set-proxy 'user:pass@proxy.example.com:3128'
  ```

Указание параметров подключения к прокси-серверу для прокси-сервера, не требующего аутентификации. Эти параметры записываются в конфигурационный файл.

- В ОС Linux:
  ```
  ./kl_feed_util --set-proxy 'proxy.example.com:3128'
  ```
- В ОС Windows:
  ```
  kl_feed_util.exe --set-proxy 'proxy.example.com:3128'
  ```

Указание параметров подключения к серверу TAXII. Эти параметры записываются в конфигурационный файл.

- В ОС Linux:
  ```
  ./kl_feed_util --set-taxii 'user:pass@Example_Feed_Name@http://example.com@Example_Collection'
  ```
- В ОС Windows:
  ```
  kl_feed_util.exe --set-taxii 'user:pass@Example_Feed_Name@http://example.com@Example_Collection'
  ```

Отображение средней скорости, с которой Feed Utility загружает потоки данных об угрозах с серверов «Лаборатории Касперского».

- В ОС Linux:
  ```
  ./kl_feed_util --speedtest
  ```
- В ОС Windows:
  ```
  kl_feed_util.exe --speedtest
  ```

Получение списка доступных потоков данных об угрозах с последующим сохранением этого списка в файле available_feeds.txt.

- В ОС Linux:
  ```
  ./kl_feed_util -l > available_feeds.txt
  ```
- В ОС Windows:
  ```
  kl_feed_util.exe -l > available_feeds.txt
  ```

Настройка Feed Utility

В этом разделе описывается порядок настройки Feed Utility.

О конфигурационном файле (Feed Utility)

Feed Utility считывает параметры из конфигурационного файла.

Редактирование конфигурационного файла

Если конфигурационный файл отсутствует или не соответствует правилам, приведенным в этом разделе, Feed Utility не запускается и выводит сообщение об ошибке.

Чтобы избежать возможных проблем, создайте резервную копию конфигурационного файла Feed Utility, прежде чем вносить в него какие-либо изменения. Если после перенастройки Feed Utility Kaspersky CyberTrace не работает должным образом, замените конфигурационный файл его резервной копией.

Расположение конфигурационного файла (Linux)

В ОС Linux конфигурационный файл, используемый Feed Utility, имеет имя `kl_feed_util.conf` и находится в каталоге `%service_dir%/etc`.

Расположение конфигурационного файла (Windows)

Конфигурационный файл, используемый Feed Utility, имеет имя `kl_feed_util.conf` и располагается в том же каталоге, что и бинарный файл Feed Utility, `%service_dir%/bin`.

Требования к кодировке

Конфигурационный файл Feed Utility, включая все указанные в нем пути, должен иметь кодировку UTF-8. Если в конфигурационном файле используются символы, не входящие в набор ASCII, и файл при этом не имеет кодировки UTF-8, Feed Utility не запустится.

Чувствительность к регистру

Все имена, используемые в конфигурационном файле (например, имена шаблонов или поля потоков данных об угрозах), чувствительны к регистру.

Использование специальных символов

Конфигурационный файл Feed Utility представляет собой файл XML. Если требуется использовать символы, зарезервированные для разметки XML (амперсанд, угловые скобки или кавычки), значение, содержащее такие символы, следует заключить в раздел CDATA.

Ниже приведен пример раздела CDATA в файле `kl_feed_util.conf`:

```
<Example><![CDATA[parameter="value"]]></Example>
```

Абсолютные и относительные пути

При определении каталогов и файлов, используемых Feed Utility, можно использовать как абсолютные, так и относительные пути. Если задан относительный путь, он вычисляется относительно каталога, в котором находится бинарный файл Feed Utility.

Параметры настройки Feed Utility

Feed Utility считывает параметры конфигурации, правила потоков данных об угрозах, правила фильтрации и правила парсинга для потоков данных об угрозах из конфигурационного файла. В этом файле в формате XML несколько групп параметров.

> Пути в конфигурационном файле должны содержать только символы, используемые в локали операционной системы, иначе Feed Utility не будет работать.

Feed (правила потоков данных об угрозах, правила фильтрации и правила парсинга)

Параметр `Feed` содержит правила для определенного потока данных об угрозах. Этот элемент имеет несколько типов вложенных параметров:

- Правила потока данных об угрозах определяют, как данный конкретный поток данных об угрозах должен обрабатываться в Feed Utility.
- Правила фильтрации — это критерии, которые Feed Utility использует для фильтрации исходных файлов потока данных об угрозах. Правила фильтрации являются составной частью правил для каждого потока данных об угрозах.
- Правила парсинга — это правила для пользовательских потоков данных об угрозах (потоков данных об угрозах OSINT и других потоков данных об угрозах, не являющихся потоками данных об угрозах Kaspersky Threat Data Feeds). Эти параметры определяют, как должен выполняться парсинг каждого потока данных об угрозах в Feed Utility.

У этого параметра есть следующие атрибуты:

- `enabled`

  Указывает, должна ли Feed Utility загружать и обрабатывать этот поток данных об угрозах.

  Если параметр `enabled` имеет значение «true», Feed Utility загружает и обрабатывает этот поток данных об угрозах. Если параметр `enabled` имеет значение «false», Feed Utility пропускает этот поток данных об угрозах.

В следующем примере показаны вложенные правила потока данных об угрозах, правила фильтрации и правила парсинга в конфигурационном файле.

```
<Settings>
    ...
    <Feeds>
    ...
        <Feed enabled="true">
           <Name>Malicious_Hash_Data_Feed</Name>
           <!-- Other feed rules for this feed -->
           <Filters>
                <Field name="popularity" value="4;5"/>
                <!-- Other filtering rules for this feed -->
           </Filters>
        </Feed>
        <Feed>
            <Name>Botnet_CnC_URL_Data_Feed</Name>
            <!-- Other feed rules for this feed -->
            <!-- This feed has no filtering rules -->
        </Feed>
    ...
    </Feeds>
    ...
</Settings>
```

FeedsDir

Параметр `FeedsDir` задает каталог, в который Feed Utility помещает обработанные файлы потоков данных об угрозах.

WorkDir

Параметр `WorkDir` задает каталог, в который Feed Utility помещает загруженные и распакованные файлы потоков данных об угрозах.

Если этот параметр не указан, Feed Utility использует временный каталог операционной системы по умолчанию.

`WorkDir` не может быть идентичным `FeedsDir`.

CertFile

Параметр `CertFile` задает путь к файлу сертификата. Этот сертификат используется Feed Utility для загрузки потоков данных об угрозах.

Файл сертификата должен иметь формат PEM.

SourceIPs

Параметр `SourceIPs` задает IP-адреса, которые используются в Feed Utility для загрузки потоков данных об угрозах.

Этот параметр является необязательным. Если он не указан или имеет пустое значение, Feed Utility использует для разрешения адресов серверов «Лаборатории Касперского» их доменные имена.

В этом параметре можно указать один или несколько IPv4-адресов. При указании нескольких IP-адресов следует использовать точку с запятой («`;`») в качестве разделителя.

В следующем примере демонстрируется указание IP-адресов в параметре `SourceIPs`.

```
<SourceIPs>192.0.2.1;192.0.2.2</SourceIPs>
```

SourceDomains

Параметр `SourceDomains` задает доменные имена, используемые Feed Utility для загрузки потоков данных об угрозах.

В этом параметре можно указать одно или несколько доменных имен. При указании нескольких доменных имен следует использовать точку с запятой («`;`») в качестве разделителя. Feed Utility будет пытаться загрузить потоки данных об угрозах с указанных доменных имен в том порядке, в котором они указаны в конфигурационном файле.

Когда параметры `SourceDomains` и `SourceIPs` используются одновременно, домены, указанные в параметре `SourceDomains`, используются прежде IP-адресов, указанных в параметре `SourceIPs`. Если все попытки загрузить потоки данных об угрозах завершились неуспешно, Feed Utility выдает сообщение об ошибке.

В этом параметре можно использовать символы Uncode.

В следующем примере демонстрируется указание IP-адресов в параметре `SourceDomains`.

```
<SourceDomains>updates1.example.com;updates2.example.com</SourceDomains>
```

CreateExternalFeedInfoList path="PATH"

> Этот параметр считается устаревшим. В текущей версии Kaspersky CyberTrace он игнорируется.

Параметр `CreateExternalFeedInfoList` указывает, должен ли создаваться список поддерживаемых потоков данных об угрозах OSINT. Этот параметр является обязательным.

Если этот параметр имеет значение `1`, Feed Utility создает список поддерживаемых потоков данных об угрозах OSINT «osint_feed_list.conf» в каталоге, указанном в атрибуте `path`. Если в Kaspersky CyberTrace были добавлены какие-либо пользовательские или сторонние потоки данных об угрозах, Feed Utility также создаст список этих потоков данных об угрозах «custom_feed_list.conf» в том же каталоге, что и «osint_feed_list.conf».

Если этот параметр имеет значение `0`, Feed Utility не создает список поддерживаемых потоков данных об угрозах OSINT.

В следующем примере демонстрируется указание пути, по которому должен быть создан список. В этом примере список создается в том же каталоге, в котором находится бинарный файл Feed Utility.

```
<CreateExternalFeedInfoList path=".">1</CreateExternalFeedInfoList>
```

NotifyKTFS path="PATH"

Параметр `NotifyKTFS` указывает, должен ли Kaspersky CyberTrace Service получать уведомления об обновлениях потоков данных об угрозах.

Этот параметр можно использовать только с форматом вывода `json`.

Если этот параметр имеет значение `1`, Feed Utility уведомляет Kaspersky CyberTrace Service о необходимости перезагрузки потоков данных об угрозах. В атрибуте `path` этого параметра должен быть указан путь к бинарному файлу Kaspersky CyberTrace Service.

Если этот параметр имеет значение `0`, Feed Utility не отправляет уведомления в Kaspersky CyberTrace Service.

EULA

Параметр `EULA` указывает, были ли приняты условия Лицензионного соглашения (EULA).

Если этот параметр имеет значение `accepted`, условия лицензионного соглашения были приняты.

Если этот параметр имеет значение `rejected`, условия лицензионного соглашения не были приняты. В этом случае использование Feed Utility невозможно.

RetryCount

Параметр `RetryCount` указывает количество попыток загрузки потока данных об угрозах Kaspersky Threat Data Feeds. Feed Utility пытается повторно загрузить поток данных об угрозах при истечении времени ожидания соединения, при частичной загрузки и при возникновении других ошибок.

Если указанное количество попыток оказалось безуспешным, Feed Utility отобразит сообщение об ошибке и продолжит работу.

> Этот параметр используется только для потоков данных об угрозах Kaspersky Threat Data Feeds. Feed Utility не загружает повторно потоки данных об угрозах OSINT и другие пользовательские потоки данных об угрозах.

Этот параметр является необязательным. Если этот параметр не указан, Feed Utility использует значение по умолчанию `10`.

Если этот параметр имеет значение `0`, количество попыток не ограничено.

SequentialDownload

Параметр `SequentialDownload` указывает, должна ли Feed Utility загружать потоки данных об угрозах в последовательном или параллельном режиме.

Если это значение равно `1` или `true`, Feed Utility загружает потоки данных об угрозах в последовательном режиме, один за другим.

Если это значение равно `0` или `false`, Feed Utility загружает потоки данных об угрозах в параллельном режиме, все одновременно.

По умолчанию этот параметр имеет значение `0`.

OutputFormat

Параметр `OutputFormat` определяет формат вывода для всех потоков данных об угрозах. Этот параметр может иметь следующие значения:

- `json`

  Потоки данных об угрозах выводятся в формате JSON. Файлы потоков данных об угрозах имеют расширение .json.

Это значение задано по умолчанию. Если параметр `OutputFormat` пропущен, для определения формата вывода используется это значение.

- `txt`

  Потоки данных об угрозах выводятся в простом текстовом формате (UTF-8 с BOM). Файлы потокjd данных об угрозах имеют расширение .txt.

  - Атрибут `delimiter`

    В этом формате поля записи разделяются разделителем. По умолчанию в качестве разделителя используется точка с запятой — «`;`». Указать собственный разделитель можно с помощью атрибута `delimiter` следующим образом:

    ```
    <OutputFormat delimiter="%delimiter%">txt</OutputFormat>
    ```

    Здесь `%delimiter%` необходимо заменить символом, который должен использоваться в качестве разделителя.

  - Атрибут `indicatorPerLine`

    Чтобы выводить по одному полю записи в строке, установите для атрибута `indicatorPerLine` значение 1 следующим образом:

    ```
    <OutputFormat indicatorPerLine="1">txt</OutputFormat>
    ```

    Если используется этот атрибут, вложенные поля, указанные в правиле потока данных об угрозах `RequiredFields`, должны иметь одно и то же родительское поле. Например, запись «`files/MD5;files/SHA1`» корректна, а запись «`files/MD5;whois/domain`» некорректна и приведет к ошибке.

  Если указан этот формат вывода, все правила потоков данных об угрозах в конфигурационном файле должны включать в себя параметр `RequiredFields`. Параметр `RequiredFields` задает порядок, в котором поля записываются в выходной поток данных об угрозах.

- `csv`

  То же, что и `txt`. Файлы потоков данных об угрозах имеют расширение .csv.

  Можно использовать атрибуты `delimiter` и `indicatorPerLine`.

- `openioc`

  Потоки данных об угрозах имеют формат OpenIOC. Файлы потоков данных об угрозах имеют расширение .ioc.

  Версию формата OpenIOC можно указатьв атрибуте `version`: это может быть `1.0` или `1.1`. Если этот атрибут не указан, используется версия `1.1`.

  Преобразование потоков данных об угрозах в формат OpenIOC 1.0 связано с некоторыми ограничениями. Потоки данных об угрозах Phishing URL Data Feed и Malicious URL Data Feed не могут быть преобразованы в формат OpenIOC 1.0; вместо этого в консоль выводится сообщение об ошибке. Для других потоков данных об угрозах конвертируются только поля хешей и IP-адресов. Конвертация потоков данных об угрозах в формат OpenIOC 1.1 не влечет таких ограничений.

  > Элемент `RequiredFields` использовать не рекомендуется. В этом случае в потоке данных об угрозах будут отсутствовать поля, обязательные для преобразования в формат OpenIOC.

  > Параметр `RecordsCount` использовать не рекомедуется, поскольку он не предназначен для этого формата. Результаты использования этого параметра могут быть непредсказуемыми.

Потоки данных об угрозах в формате OpenIOC занимают значительно больше места на жестком диске, чем исходные файлы потоков данных об угрозах.

- `stix`

  Потока данных об угрозах имеют формат STIX™. Файлы имеют расширение .xml.

  Для формата STIX потоки данных об угрозах с масками URL должны иметь поле `type`.

  Версию формата STIX можно указать в атрибуте `version`: это может быть `1`, `2.0` или `2.1`. Если указано значение `1`, поток данных об угрозах выводится в формате STIX 1.1. Если атрибут не указан, используется значение `1`.

  Элемент `RequiredFields` использовать не рекомендуется. В этом случае в потоке данных об угрозах будут отсутствовать поля, обязательные для преобразования в формат STIX.

  Параметр `RecordsCount` использовать не рекомедуется, поскольку он не предназначен для этого формата. Результаты использования этого параметра могут быть непредсказуемыми.

  Потоки данных об угрозах в формате STIX занимают значительно больше места на жестком диске, чем исходные файлы потоков данных об угрозах.

В следующем примере показан вложенный параметр `OutputFormat` в конфигурационном файле.

```
<Settings>
    ...
    <Feeds>
        <OutputFormat>json</OutputFormat>
        ...
    </Feeds>
    ...
</Settings>
```

CreateDiff

Параметр `CreateDiff` указывает, должна ли Feed Utility создавать *инкрементные части для потоков данных об угрозах*. Инкрементные потоки данных об угрозах — это файлы, содержащие различия между старой и новой версиями обрабатываемого файла потока данных об угрозах. Этот параметр влияет на все потоки данных об угрозах, создаваемые Feed Utility, следующим образом:

- Если этот параметр имеет значение `0`, Feed Utility не создает инкрементные потоки данных об угрозах. Это значение задано по умолчанию.

- Если этот параметр имеет значение `1`, Feed Utility создает инкрементные потоки данных об угрозах.

Если для параметра `CreateDiff` задано значение `1` и загружаются новые версии потоков данных об угрозах, для каждого потока данных об угрозах создаются два дополнительных файла (`%feed_name%` — имя файла потока данных об угрозах):

- Файл `%feed_name%_new.json` содержит записи, которые были добавлены в новую версию файла потока данных об угрозах.
- Файл `%feed_name%_del.json` содержит записи, которые были удалены в новой версии файла потока данных об угрозах.

Инкрементные потоки данных об угрозах можно создавать только для потоков данных об угрозах в формате JSON, содержащихся в одном файле:

- Параметр `OutputFormat` должен иметь значение `json`.
- Для каждого потока данных об угрозах параметр `UrlMatcherField` должен быть опущен или иметь пустое значение.
- Для каждого потока данных об угрозах параметр `RecordsCount` не должен иметь атрибута `perFile` или этот атрибут должен иметь значение `0`.

Для создания инкрементного потока данных об угрозах Feed Utility использует ключевое поле в старой и новой версиях потока данных об угрозах:

- Если этот поток данных об угрозах содержит невложенные поля `id`, `MD5`, `ip`, `url` или `domain`, это поле используется как ключевое поле.
- Если все вышеперечисленные поля отсутствуют, Feed Utility пытается найти в потоке данных об угрозах поле с уникальными значениями. Если эта попытка не удалась, выдается предупреждение.

В следующем примере показан вложенный параметр `OutputFormat` в конфигурационном файле.

```
<Settings>
    ...
    <Feeds>
        ...
        <CreateDiff>0</CreateDiff>
        ...
    </Feeds>
    ...
</Settings>
```

ProxySettings

Параметр `ProxySettings` задает настройки прокси-сервера для Feed Utility. Если указан прокси-сервер, Feed Utility загружает потоки данных об угрозах с использованием указанных параметров.

Имя пользователя и пароль для прокси-сервера хранятся в конфигурационном файле Feed Utility. Эта информация не передается в «Лабораторию Касперского».

Настройки прокси задаются в следующих параметрах:

- `Host`

  Хост прокси-сервера.

  В этом параметре можно указать доменное имя или IP-адрес. Поддерживаются адреса IPv4 и IPv6.

- `Port`

  Порт прокси-сервера.

- `User`

  Зашифрованное имя пользователя для аутентификации на прокси-сервере.

  Если прокси-сервер не требует аутентификации, оставьте этот параметр пустым.

  > Этот параметр хранится в зашифрованном виде. Для установки этого параметра используется параметр командной строки `--set-proxy`. Если вместо использования этого параметра командной строки ввести имя пользователя в незашифрованном виде, соединение с прокси-сервером не будет установлено.

- `Password`

  Зашифрованный пароль для аутентификации на прокси-сервере.

  Если прокси-сервер не требует аутентификации, оставьте этот параметр пустым.

  > Этот параметр хранится в зашифрованном виде. Для установки этого параметра используется параметр командной строки `--set-proxy`. Если вместо использования этого параметра командной строки ввести пароль в незашифрованном виде, соединение с прокси-сервером не будет установлено.

В следующем примере показаны вложенные параметры прокси-сервера в конфигурационном файле.

```
<Settings>
    ...
    <ProxySettings>
        <Host></Host>
        <Port></Port>
        <User></User>
        <Password></Password>
    </ProxySettings>
    ...
</Settings>
```

LogSettings

Параметр `LogSettings` определяет, каким образом Feed Utility ведет свой журнал.

Если ведение журнала включено, Feed Utility может записывать в файлы журнала любые из следующих сведений, которые могут считаться конфиденциальными, относящимися к безопасности или чувствительными: параметры конфигурации Feed Utility, хост и порт прокси-сервера, а также операции, выполняемые при загрузке и обработке потоков данных об угрозах.

> Если ведение журнала включено, Feed Utility записывает в файлы журнала информацию о свободном месте на жестком диске, доступном для рабочих каталогов и каталогов потоков данных об угрозах. Также, начиная с этой версии, в журналы будет записываться средняя скорость загрузки потоков данных об угрозах.

Файлы журнала представляют собой простые текстовые файлы. Вся информация записывается в файлы журнала в незашифрованном виде. Файлы журнала имеют стандартные унаследованные права доступа. Рекомендуется назначить каталогу для хранения файлов журнала соответствующие права, чтобы читать файлы журнала мог только администратор.

Файлы журнала хранятся до тех пор, пока они не будут явным образом удалены пользователем.

Feed Utility не отправляет файлы журналов или какие-либо данные, содержащиеся в них, в «Лабораторию Касперского». В целях оказания технической поддержки ваш менеджер по работе с клиентами может попросить вас предоставить файлы журнала.

Настройки ведения журнала задаются в следующих параметрах:

- `EnableLog`

  Включение ведения журнала.

  Если это значение равно `1` или `true`, Feed Utility ведет журнал своих действий.

  Если это значение равно `0` или `false`, Feed Utility не ведет журнал своих действий.

- `LogsDir`

  Каталог, в котором Feed Utility хранит свои файлы журналов.

- `CleanOldLog`

  Позволяет удалять старые файлы журналов.

  Если это значение равно `0`, при инициализации Feed Utility сохраняет старые файлы журналов.

  Если это значение равно `1`, при инициализации Feed Utility удаляет старые файлы журналов.

В следующем примере показаны вложенные настройки ведения журнала в конфигурационном файле.

```
<Settings>
    ...
    <LogSettings>
        <EnableLog>0</EnableLog>
        <LogsDir>logs</LogsDir>
        <CleanOldLog>1</CleanOldLog>
    </LogSettings>
</Settings>
```

Правила потоков данных об угрозах

Способ обработки каждого конкретного потока данных об угрозах в Feed Utility, определяется правилами, заданными для потоков данных об угрозах в элементах `Feed`.

По умолчанию в конфигурационном файле присутствуют записи, содержащие правила для всех потоков данных об угрозах. Записи для коммерческих потоков данных об угрозах отключены. Если для скачивания потоков данных об угрозах используется коммерческий сертификат, следует раскомментировать записи потоков данных об угрозах, доступных с используемым сертификатом.

Пример правил потока данных об угрозах

Ниже приведен пример правил потока данных об угрозах. Правила потока данных об угрозах указываются индивидуально для каждого потока данных об угрозах.

```
<Settings>
    ...
    <Feeds>
        <Feed enabled="true">
            <Name>Botnet_CnC_URL_Data_Feed</Name>
            <FeedID>65</FeedID>
            <Filters>
                <Field name="geo" value="RU"/>
            </Filters>
            <UrlMatcherField toRegex="false">mask</UrlMatcherField>
            <RequiredFields>mask;geo;first_seen;last_seen</RequiredFields>
            <RecordsCount perFile="100" total="1000" />
            <FeedFields/>
        </Feed>
        <Feed enabled="false">
            <Name>CustomFeed</Name>
            <Path>./custom_example/example_feed.json</Path>
            <Parsing type="json">
                <MD5 type="MD5">files/MD5</MD5>
            </Parsing>
            <FeedFields/>
        </Feed>
        ...
    </Feeds>
    ...
</Settings>
```

Feed

Этот родительский элемент содержит правила для определенного потока данных об угрозах.

Имя

Этот элемент задает имя загруженного файла потока данных об угрозах.

После того, как Feed Utility распаковывает загруженные потоки данных об угрозах, выполняется поиск файла с именем, начинающимся с указанной строки. Если указанная строка присутствует в начале имен нескольких файлов, Feed Utility выводит сообщение об ошибке и прекращает обработку потоков данных об угрозах. В этом случае необходимо вручную разрешить этот конфликт, например, путем удаления лишних файлов из каталога, в который Feed Utility их распаковывает. Этот каталог задается параметром `WorkDir`.

В значении этого параметра регистр не учитывается.

Значение этого параметра должно быть уникальным. У каких-либо двух элементов `Feed` не должно быть одинакового значения этого параметра.

FeedID

Этот элемент применяется только к потокам данных об угрозах «Лаборатории Касперского».

Этот элемент задает идентификатор потока данных об угрозах. Feed Utility использует этот параметр для загрузки потоков данных об угрозах с серверов обновлений.

Атрибут `enabled` указывает, должна ли Feed Utility обрабатывать этот поток данных об угрозах:

- Если этот атрибут имеет значение `true`, Feed Utility обрабатывает соответствующий поток данных об угрозах.
- Если этот атрибут имеет значение `false`, Feed Utility пропускает соответствующий поток данных об угрозах.

Path

Параметр `Path` задает путь и имя файла для пользовательского или стороннего потока данных об угрозах.

Поддерживаются следующие типы значений:

- Путь и имя файла на том сервере, где находится бинарный файл Feed Utility.
- Путь и имя файла FTP или FTPS.
- URL HTTP или HTTPS.
- Сетевой путь (поддерживается только в операционной системе Windows).

У этого параметра есть следующие атрибуты:

- cert

  Задает путь к сертификату, который будет использоваться для загрузки этого потока данных об угрозах по HTTPS или FTPS. Этот атрибут не является обязательным. Если атрибут не указан, Feed Utility не использует сертификат.

Тип аутентификации указывается в параметре `Settings > Feeds > Feed` конфигурационного файла Feed Utility.

Для потока данных типа «электронная почта» выберите протокол соединения, указав для атрибута «type» значение «POP3» или «IMAP».

Если выбран протокол соединения, укажите в элементе Path «IPv4/Host name» и порт почтового сервера.

Authorization

Базовые параметры аутентификации для пользовательских или сторонних потоков данных об угрозах.

У этого параметра есть два вложенных элемента:

- `User`

  Зашифрованное имя пользователя для базовой аутентификации на сервере, с которого загружаются потоки данных об угрозах.

  Для установки этого параметра используется параметр командной строки `--set-basic-auth`. Для потоков данных об угрозах STIX, загружаемых с сервера TAXII™, используется параметр `--set-taxii`.

  Этот элемент не может быть пустым.

- `Password`

  Зашифрованный пароль для базовой аутентификации на сервере, с которого загружаются потоки данных об угрозах.

  Для установки этого параметра используется параметр командной строки `--set-basic-auth`. Для потоков данных об угрозах STIX, загружаемых с сервера TAXII™, используется параметр `--set-taxii`.

Если этот тип аутентификации не требуется, не указывайте этот параметр.

TAXII

Параметр TAXII указывает расположение потока данных об угрозах STIX. Этот элемент должен содержать адрес службы опроса (Poll) сервера TAXII.

У этого параметра есть следующие атрибуты:

- `collection_name`

  Название коллекции данных для этого потока данных об угрозах STIX.

- `version`

  Версия сервера TAXII. Возможные значения этого атрибута: `1`, `2.0` и `2.1`. Для потока данных об угрозах STIX 2.0 необходимо указать сервер TAXII 2.0. Для потока данных об угрозах STIX 2.1 необходимо указать сервер TAXII 2.1.

  По умолчанию значение этого атрибута равно `1`.

В следующем примере демонстрируется указание местоположения потока данных об угрозах STIX:

```
<TAXII collection_name="example-collection" version="2.1">http://192.0.2.10:9000</TAXII>
```

Настройка авторизации на сервере TAXII

Учетные данные для авторизации на сервере TAXII.

У этого параметра есть два вложенных элемента:

- `User`

  Имя пользователя для авторизации на сервере TAXII.

  Этот параметр хранится в зашифрованном виде. Для установки этого параметра используется параметр командной строки `--set-taxii`. Если вместо использования этого параметра командной строки ввести имя пользователя в незашифрованном виде, соединение с сервером TAXII не будет установлено.

- `Password`

  Пароль для авторизации на сервере TAXII.

  Этот параметр хранится в зашифрованном виде. Для установки этого параметра используется параметр командной строки `--set-taxii`. Если вместо использования этого параметра командной строки ввести пароль в незашифрованном виде, соединение с сервером TAXII не будет установлено.

Следующий пример демонстрирует использование этого параметра:

```
<Feed>
    <Name>TAXII</Name>
    <TAXII collection_name="example-collection" version="2.1">http://192.0.2.10:9000</TAXII>
    <Authorization>
        <User>zQYq33rAY7dgImLtk8W0jQ==</User>
        <Password>OUYWpkPDoH+vv/IFfCrshw==</Password>
    </Authorization>
</Feed>
```

Filters

Этот элемент задает правила фильтрации для потока данных об угрозах. Каждое правило фильтрации определяется в отдельном элементе `Field`.

Этот элемент не является обязательным. Если элемент не содержит вложенных элементов `Field`, Feed Utility ведет себя так, как будто элемент `Filters` пропущен. Если элемент `Filters` отсутствует, фильтрация не производится.

UrlMatcherField

Этот элемент определяет способ обработка в Feed Utility потоков данных об угрозах с масками URL.

Если Feed Utility используется как часть Kaspersky CyberTrace вместе с Kaspersky CyberTrace Service, потоки данных, содержащие маски URL, должны быть преобразованы в двоичный формат.

> Если Feed Utility используется отдельно от Kaspersky CyberTrace Service, нет необходимости компилировать маски, поэтому в таком случае элемент `UrlMatcherField` может отсутствовать в конфигурационном файле Feed Utility.

Этот элемент имеет значение и необязательный атрибут `toRegex`:

- Значение элемента определяет имя поля в потоке данных об угрозах, содержащее маску URL.
- Необязательный атрибут `toRegex` этого элемента определяет, как утилита должна обрабатывать поток данных об угрозах.
  - Если атрибут `toRegex` имеет значение `0`, `false` или не указан, Feed Utility компилирует поток данных об угрозах и создает двоичные файлы, которые могут использоваться в Kaspersky CyberTrace Service.
  - Если атрибут `toRegex` имеет значение `1` или `true`, приложение Feed Utility обрабатывает маски URL в потоках данных об угрозах, преобразовывая их в регулярные выражения.

    Для каждой маски URL в Feed Utility создается регулярное выражение, сопоставляющее все URL, охватываемые данной маской URL. Например, маске URL `botnet.example.com` соответствует регулярное выражение `((\/{2}|^)botnet\.example\.com(\/.*|$))`. Как и маска URL, это регулярное выражение сопоставляет все URL домена `botnet.example.com`.

    Атрибут `toRegex` может иметь значение `1` только для тех потоков данных об угрозах, у которых есть поле `type`. Кроме того, если среди правил потока данных об угрозах присутствует элемент `RequiredFields`, он должен содержать поле `type`.

В случае формата вывода `json` можно принять следующие меры:

- Компиляция потоков данных об угрозах с масками URL в двоичный файл, который может использовать Kaspersky CyberTrace Service.

  Если используется Kaspersky CyberTrace Service, элемент `UrlMatcherField` является обязательным для потоков данных об угрозах, содержащих маски URL: «Malicious URL Feed», «Phishing URL Feed», «Botnet C&C URL Feed» и «IoT URL Feed».

  ```
  <UrlMatcherField>%field_name%</UrlMatcherField>
  ```

- Преобразование масок URL в регулярные выражения.

  ```
  <UrlMatcherField toRegex=1>%field_name%</UrlMatcherField>
  ```

- Отказ от конвертации масок URL.

  Не указывайте элемент `UrlMatcherField`.

В случае выходных форматов `csv` и `txt` можно принять следующие меры:

- Преобразование масок URL в регулярные выражения.

  `<UrlMatcherField toRegex=1>%field_name%</UrlMatcherField>`

- Отказ от конвертации масок URL.

  Не указывайте элемент `UrlMatcherField`.

В случае выходных форматов `openioc` и `stix` этот элемент не следует указывать. Этот элемент невозможно использовать с этими выходными форматами.

RequiredFields

Этот элемент определяет поля, которые включаются в обработанный поток данных об угрозах. Этот элемент является обязательным для выходных форматов `txt` и `csv`. Если элемент `RequiredFields` не указан, в обработанный поток данных об угрозах попадают все поля записи.

Имена полей разделяются точкой с запятой («`;`»). Косая черта («`/`») в имени поля указывает на вложенное поле (в смысле формата JSON).

Этот элемент определяет поля в итоговом потоке данных об угрозах; это работает не как правило фильтрации. Например, если для потока данных об угрозах определено правило `<RequiredFields>id;mask</RequiredFields>`, в записях в обрабатываемом потоке данных об угрозах присутствуют только поля `id` и `mask`. Также будут включены записи, в которых есть хотя бы одно из указанных полей (`id` или `mask`). Записи, в которых нет хотя бы одного из указанных полей, будут исключены, поскольку отсутствие указанных полей приводит к добавлению пустой записи в обрабатываемый поток данных об угрозах. Если требуется отфильтровать поток данных об угрозах так, чтобы в итоговый поток данных об угрозах включались только записи, содержащие все указанные поля, необходимо использовать правила фильтрации. Сведения об использовании элемента `RequiredFields` одновременно с критериями фильтрации приведена в подразделе «Исключение записей с пропущенными полями» в разделе Правила фильтрации.

Поля записи записываются в форматы `csv` и `txt` в том порядке, в котором они указаны в элементе `RequiredFields`. Поля записи записываются в формате `json` в том порядке, в котором они встречаются в исходном потоке данных об угрозах. В случае форматов `openioc` и `stix` порядок записей не определен; записи выводятся в порядке обработки.

FeedFields

В этом элементе перечислены все поля, присутствующие в потоке данных об угрозах.

> Не изменяйте этот параметр. Feed Utility автоматически записывает в него значения полей.

RecordsCount

Этот элемент задает максимальное количество записей, которые будут включены в обрабатываемый поток данных об угрозах.

У этого элемента есть два атрибута.

- Атрибут `total` этого элемента определяет общее количество записей первого уровня, которые должны быть включены в обрабатываемые файлы. Feed Utility включает только те записи, которые соответствуют правилам фильтрации. Если это значение равно `0`, это количество не ограничено и включаются все записи.

  Обратите внимание, что атрибут `total` относится к записям первого уровня, поэтому обработанный поток данных об угрозах может содержать больше вложенных записей, чем предусматривает значение `total`. Например, пусть исходный поток данных об угрозах содержит следующие данные:

  ```
  [
  {
    "time": "23.02.1992 15:43",
    "urls":[
         {
            "url" : "http://url.biz/sample1"
         },
         {
            "url" : "http://url.biz/sample2"
         }
     ]
   },
  {
    "time": "24.02.1992 15:43",
    "urls":[
         {
            "url" : "http://url.biz/sample3"
         },
         {
            "url" : "http://url.biz/sample4"
         }
     ]
   }
  ]
  ```

  Для этого потока данных об угрозах можно задать следующие настройки в конфигурационном файле Feed Utility:

  ```
  <OutputFormat>csv</OutputFormat>
  <RequiredFields>urls/url</RequiredFields>
  <RecordsCount total="1" />
  ```

  Обработанный поток данных об угрозах будет содержать две записи, поскольку они вложены в одну запись первого уровня.

  ```
  http://url.biz/sample1
  http://url.biz/sample2
  ```

- Атрибут `perFile` этого элемента определяет максимальное количество записей, которые должны быть включены в один файл. Если общее количество записей в одном обработанном файле потока данных об угрозах превышает это значение, Feed Utility создает дополнительный файл потока данных об угрозах.

  Например, если атрибут `total` имеет значение `1000`, а `perFile` имеет значение `300`, при этом Feed Utility обнаруживает 650 записей, соответствующих правилам фильтрации, то создаются три файла (два файла по 300 записей и один файл с 50 записями).

  Этот атрибут нельзя использовать в следующих случаях:

  - Атрибут `perFile` нельзя использовать для потоков данных об угрозах с масками URL, которые скомпилированы в двоичный формат.

  - Атрибут `perFile` нельзя использовать с пользовательскими потоками данных об угрозах, для которых определены правила парсинга, в которых для атрибута `type` заданы типы `url` или `domain`. Такие потоки данных об угрозах также компилируются в двоичный формат с помощью Feed Utility. Чтобы использовать атрибут `perFile` для полей этих типов, необходимо изменить тип поля на `context`.

Parsing

Этот элемент содержит правила парсинга для пользовательских потоков данных об угрозах.

Правила для потоков данных об угрозах типа «электронная почта»

Feed Utility может загружать сторонние потоки данных об угрозах типа «электронная почта» с почтового сервера.

Настройте подключение к почтовому серверу в следующих элементах конфигурационного файла `kl_feed_util`:

- `MailboxConnection`

  Этот элемент является обязательным, если в элементе `Path` включены протоколы POP3/IMAP.

  У этого элемента есть следующие атрибуты:

  - `use_tls`

    Значения `true` и `false` для атрибута `use_tls` включают или выключают использование TLS/SSL для взаимодействия с почтовым сервером. По умолчанию задано значение `true`.

  - `receive_period`

    Максимальное значение этого атрибута равно 360, предустановлено значение 7, минимально возможное значение равно 1.

    Feed Utility обрабатывает только сообщения электронной почты, полученные после последнего обновления потока данных об угрозах типа «электронная почта».

    Если поток данных об угрозах электронной почты ранее не обновлялся, Feed Utility обрабатывает все сообщения электронной почты за количество дней, указанное в атрибуте `receive_period`.

- `MailboxConnection/User`

  Значение этого элемента закодировано. Для подключения к почтовому серверу Feed Utility кодирует имя пользователя с помощью параметра `--set-mailbox`.

- `MailboxConnection/Password`

  Значение этого элемента закодировано. Для подключения к почтовому серверу Feed Utility кодирует пароль с помощью параметра `--set-mailbox`.

  > Для проверки соединения с почтовым сервером используется атрибут --check-mailbox-connection.

- `MailboxConnection/Filters`

  В этом разделе можно указать одно или несколько правил фильтрации сообщений почтового сервера. Этот раздел не является обязательным. Более подробные сведения приведены в разделе Правила фильтрации.

- `Parsing`

  Порядок задания правил парсинга для потока данных об угрозах типа «электронная почта» приведен в разделе Правила парсинга.

В следующем примере демонстрируются настройки подключения к почтовому серверу:

```
 <Feed enabled="true">
    <Name>Email_OSINT</Name>
    <Path type="pop3">myemailserv.com:3125</Path>
    <MailboxConnection use_tls="false" receive_period="7">
         <User>==asd</User>
          <Password>==ewq</Password>
          <Filters>
               <Filter field="from" condition="not_match">mywife@ya.ru</Filter>
               <Filter field="subject" condition="contains">Best IoCs ever</Filter>
          </Filters>
    </MailboxConnection>
    <Parsing type="messageBody">
        <ip type="ip">(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})</ip>
    </Parsing>
    <Parsing type="messageAttach">
         <Attach type="csv">
              <ip type="ip">1</ip>
        </Attach>
        <Attach type="pdf">
             <url type="url">1</url>
        </Attach>
    </Parsing>
    <Excluded>
         <Item>VALUE1</Item>
         <Item>VALUE2</Item>
    </Excluded>
</Feed>
```

Правила фильтрации

Правила фильтрации — это критерии, которые Feed Utility использует для фильтрации исходных файлов потока данных об угрозах.

Правила фильтрации для каждого потока данных об угрозах задаются в элементе `Filters`. Каждое правило фильтрации задается в элементе `Field`: имя поля указывается в атрибуте `name`, а критерии фильтрации указываются в атрибуте `value`. С полем может быть связано только одно правило фильтрации; для одного поля невозможно задать два параметра `Field`.

Потоки данных об угрозах типа «электронная почта» дополнительно фильтруются по теме письма и по отправителю. См. раздел «Правила фильтрации потоков данных об угрозах типа „электронная почта“» ниже.

Ниже приведен пример правил фильтрации для потока данных об угрозах. Эти правила определяют, что выходной поток данных об угрозах должен включать только записи со значением поля `popularity`, равным `4` или `5`, и значением поля `mask`, содержащим `.ru` или `.com`.

```
<Feed>

…

    <Filters>
        <Field name="popularity" value="4;5"/>
        <Field name="mask" value=".ru;.com"/>
    </Filters>
    ...
<Feed>
```

Feed Utility игнорирует символы пробела и табуляции в начале и в конце значения атрибута `value`.

В выходной файл включаются только те записи, которые соответствуют всем указанным критериям. Если для поля указан критерий фильтрации и при этом поле отсутствует в записи, Feed Utility не включает такую запись в выходной файл.

Определение критериев фильтрации для числовых значений

Числовые значения могут быть только целыми. Десятичные дроби не поддерживаются.

Критерии фильтрации для числовых полей можно задать следующими способами:

- `value="*"`

  Поле может иметь любое значение.

  Например, `<Field name="type" value="*"/>` означает, что поле `type` может иметь любое значение.

- `value="%value%"`

  Точное числовое значение. Поле должно быть строго равно `%value%`.

  Например, `<Field name="popularity" value="1"/>` означает, что поле `popularity` должно быть равно `1`.

- `value="%value1%;%value2%"`

  Одно из нескольких числовых значений. Поле может иметь одно из указанных числовых значений (`%value1%` или `%value2%`).

  При указании дополнительных значений в качестве разделителя используется точка с запятой («`;`»).

  Например, `<Field name="popularity" value="1;3"/>` означает, что поле `popularity` должно иметь значение `1` или `3`, но не `2`.

- `value="[%value1%;%value2%]"`

  Диапазон числовых значений.

  Поле может иметь одно из значений в указанном диапазоне от `%value1%` до `%value2%`.

  Например, `<Field name="popularity" value="[1;3]"/>` означает, что поле `popularity` должно иметь значение от `1` до `3`, в том числе `2`.

- `value="[%value1%;*]"` или `value="[*;%value1%]"`

  Открытый диапазон числовых значений. То же, что и диапазон, но звездочка (`*`) обозначает бесконечность.

  Например, `<Field name="popularity" value="[2;*]"/>` означает, что значение поля `popularity` должно быть больше или равно `2`.

Определение критериев фильтрации для строк

Критерии фильтрации для строк можно задать следующими способами:

- `value="*"`

  Поле может иметь любое значение.

  Например, `<Field name="mask" value="*"/>` означает, что поле `mask` может иметь любое значение.

- value="`%string%`"

  Поле должно содержать указанную строку.

  Например, `<Field name="geo" value="ru"/>` означает, что значение поля `geo` должно содержать «`ru`».

- `value="%string1%;%string2%"`

  Содержит одну или несколько указанных строк.

Например, `<Field name="geo" value="ru;us"/>` означает, что значение поля `geo` должно содержать «`ru`» или «`us`» либо одновременно «`ru`» и «`us`».

Определение критериев фильтрации для дат

Значения дат в потоках данных об угрозах форматируются по шаблону «`DD.MM.YYYY`» (например, «`26.04.2014`»), по шаблону «`YYYY-MM-DD`» (например, «`2014-04-26`»), либо по шаблону «`MM/DD/YYYY`» (например, «`04/26/2014`»).

Критерии фильтрации для дат можно задать следующими способами:

- `value="*"`

  Поле может иметь любое значение.

  Например, `<Field name="last_seen" value="*"/>` означает, что поле `last_seen` может иметь любое значение.

- `value="%date%"`

  Поле должно содержать указанную дату.

  Например, `<Field name="first_seen" value="14.10.2015"/>` означает, что поле `first_seen` должно иметь значение «14 октября 2015 г.».

- `value="[%date1%;%date2%]"`

  Поле должно содержать дату в указанном диапазоне.

  Например, `<Field name="first_seen" value="[01.02.2013;01.02.2015]"/>` означает, что значение поля `first_seen` должно попадать в диапазон от 1 февраля 2013 г. до 1 февраля 2015 г.

- `value="[%date1%;*]"` или `value="[*;%date1%]"`

  Открытый диапазон дат. То же, что и диапазон дат, то есть `value="[%date1%;%date2%]"`. Однако звездочка (`*`) означает бесконечность.

  Например, `<Field name="first_seen" value="[*;10.12.2015]"/>` означает, что дата в поле `first_seen` должна быть раньше или равна 10 декабря 2015 г.

Исключение записей с пропущенными полями

В исходных файлах потоков данных об угрозах некоторые записи могут иметь дополнительные поля или не иметь некоторых полей. В случае записей с дополнительными полями Feed Utility включает только те поля, которые указаны в элементе `RequiredFields` правил потока данных об угрозах для указанного потока данных об угрозах. В случае записей, в которых отсутствуют некоторые поля, Feed Utility включает такие записи в вывод, если они содержат хотя бы одно из полей, указанных в элементе `RequiredFields`. Если некоторые поля, указанные в элементе `RequiredFields`, отсутствуют в записи исходного потока данных об угрозах, запись в обработанном потоке данных об угрозах также не будет их содержать.

Если требуется исключить из вывода записи с недостающими полями, необходимо создать правила фильтрации для всех обязательных полей.

В следующем примере Feed Utility будет включать записи, в которых есть поле `popularity`, поле `mask` либо поля `popularity` и `mask` одновременно.

```
<RequiredFields>popularity;mask</RequiredFields>
```

Если требуется, чтобы Feed Utility включала в вывод только те записи, у которых есть как поле `popularity`, так и поле `mask`, необходимо создать правило фильтрации для обоих полей. Можно указать критерии для значений полей или использовать звездочку `(*)`, означающую любое значение.

В следующем примере в итоговый поток данных об угрозах включаются только записи, содержащие оба поля (`mask` и `popularity`).

```
<Filters>
    <Field name="popularity" value="*"/>
    <Field name="mask" value="*"/>
</Filters>
<RequiredFields>popularity;mask</RequiredFields>
```

Таким же образом можно указать точные критерии. В следующем примере Feed Utility должна включать только записи, в которых в поле `popularity` указано значение `5`, а в поле `mask` указано любое значение.

```
<Filters>
    <Field name="popularity" value="5"/>
    <Field name="mask" value="*"/>
</Filters>
<RequiredFields>popularity;mask</RequiredFields>
```

Правила фильтрации потоков данных об угрозах типа «электронная почта»

В конфигурационном файле kl_feed_util укажите одно или несколько правил фильтрации в элементе `MailboxConnection/Filters`. Этот элемент не является обязательным.

Если добавлено хотя бы одно правило фильтрации, укажите следующие атрибуты в элементе `MailboxConnection/Filters/Filter`:

- field

  Укажите значение `subject` (тема сообщения электронной почты) и/или значение `from` (отправитель сообщения электронной почты).

  > Почтовый сервер может хранить поле `From` в двух вариантах: sender@mail.ru или sender<sender@mail.ru>. Если в элементе Filter атрибут `condition` имеет значение `match`, значение сравнивается со значением `sender@mail.ru` (если в поле `From` содержится «sender@mail.ru»), либо значение сравнивается со значением в скобках (если в поле `From` содержится «sender<sender@mail.ru>»).

- condition

  Задаются следующие значения условий фильтрации:

  - `contains` (значение из сообщения электронной почты должно содержать значение из этого поля).
  - `not_contains` (значение из сообщения электронной почты не должно содержать значения из этого поля).

    Фильтр `not_contains` имеет приоритет над фильтром `contains`.

    Значения сравниваются без учета регистра.
  - `match` (значение из сообщения электронной почты должно совпадать со значением в этом поле).
  - `not_match` (значение из сообщения электронной почты не должно совпадать со значением в этом поле).

Ниже приведен пример правил фильтрации для потока данных об угроза типа «электронная почта»:

```
<Filters>
     <Filter field="from" condition="not_match">techsupport@ya.ru</Filter>
     <Filter field="subject" condition="contains">Best IoCs ever</Filter>
</Filters>
```

Правила парсинга

Правила парсинга задаются для пользовательских потоков данных об угрозах (потоков данных об угрозах, определенных с помощью элемента `Path`). Эти параметры определяют, как должен выполняться парсинг каждого потока данных об угрозах в Feed Utility.

Правила парсинга определяются в элементе `Parsing` правил пользовательского потока данных об угрозах.

Ниже приведен пример правил парсинга для пользовательского потока данных об угрозах. Эти правила указывают, что входной поток данных об угрозах имеет формат JSON. Правило парсинга MD5 определяется для поля `files/md5` во входном потоке данных об угрозах. Значения в этом поле проходят парсинг как хеши MD5.

```
<Feed>
    ...
    <Parsing type="json">
        <MD5 type="MD5">files/md5</MD5>
    </Parsing>
    ...
<Feed>
```

Элемент «Parsing»

Родительский элемент `Parsing` содержит все вложенные правила парсинга. Его атрибуты определяют формат входных данных.

У этого элемента есть следующие атрибуты:

- `type`

  Задает тип входного потока данных об угрозах.

  Этот атрибут может иметь следующие значения: `json`, `csv`, `xml`, `misp`, `stix`, `stix2`, `pdf`, `messageBody`, `messageAttach`.

  > Feed Utility поддерживает STIX версий 1.0, 1.1, 2.0 и 2.1. Конкретная версия STIX определяется автоматически.

  > Файл, добавленный в каталог потока данных об угрозах pdf, не обрабатывается, если этот файл создан раньше или одновременно с последним созданным файлом, который уже был обработан.

- `delimiter`

  Задает разделитель для входных потоков данных об угрозах CSV. По умолчанию используется точка с запятой (« `;` »).

- `rootElement`

Задает путь к корневому элементу для входных потоков данных об угрозах XML и JSON.

- Входные потоки данных об угрозах в формате XML

  Подстановочные знаки «*» и «? » можно использовать вместо любого другого символа или группы символов. Подстановочный знак «*» используется для группы символов. Подстановочный знак «?» используется для одиночного символа.

  Части пути `rootElement` нельзя указывать только с помощью подстановочных знаков. Например, запись «`Feeds/*/Contents`» некорректна.

- Входные потоки данных об угрозах в формате JSON

  Значение корневого элемента можно указать с любым уровнем вложенности. Пределы уровня вложенности задаются с помощью символа «/».

  Параметр «Root element» может быть пустым. Если он не пустой, значение корневого элемента не должно содержать пустых уровней вложенности (подстрока «//»), а также не должно начинаться или заканчиваться символом «/».

  В корневом элементе для потоков данных об угрозах JSON нельзя использовать подстановочные знаки.

В следующем примере демонстрируется использование элемента `Parsing` для входного потока данных об угрозах в формате XML. В этом случае правила парсинга применяются к элементам, вложенным в элемент `Feeds > Example > Contents`.

```
<Feed>
    ...
    <Parsing type="xml" rootElement="Feeds/Example/Contents">
       ...
    </Parsing>
    ...
<Feed>
```

Индивидуальные правила парсинга

Правила парсинга для отдельных полей входного потока данных об угрозах должны быть вложены в элемент `Parsing`. Когда Feed Utility обрабатывает входной поток данных об угрозах, поля выходного потока данных об угрозах создаются в соответствии с этими правилами.

Каждое правило имеет следующий формат:

```
<%OUTPUT_NAME% type="%VALUE_TYPE%">%INPUT_NAME%</%OUTPUT_NAME%>
```

Выше используются следующие элементы имени правила:

- %OUTPUT_NAME% определяет имя поля в выходном потоке данных об угрозах. Например, если %OUTPUT_NAME% — это «MD5», поле с этим значением в выходном потоке данных об угрозах также будет называться MD5.

  %OUTPUT_NAME% сохраняет вложенные поля. Если поле, указанное в %INPUT_NAME%, является вложенным, поле в выходном потоке данных об угрозах также будет вложенным. Например, если %OUTPUT_NAME% — это «MD5_HASH», а %INPUT_NAME% — это «files/md5», то поле в выходном потоке данных об угрозах будет называться «files/MD5_HASH».

  В случае входного потока данных об угрозах в формате JSON в %OUTPUT_NAME% всегда должно использоваться значение `Field`. Feed Utility использует имена полей из исходного потока данных об угрозах.

- %VALUE_TYPE% — это тип значений, хранящихся в этом поле.

Feed Utility будет обрабатывать эти значения в соответствии с указанным типом. Например, если выходной поток данных об угрозах содержит доменные имена и URL, он будет скомпилирован в двоичный формат.

Возможны следующие типы значений:

- `url` – тип значения, используемый для URL.
- `ip` – тип значения, используемый для IP-адресов.
- `md5` – тип значения, используемый для хешей MD5.
- `sha1` – тип значения, используемый для хешей SHA1.
- `sha256` – тип значения, используемый для хешей SHA256.
- `domain` – тип значения, используемый для доменных имен.
- `context` – тип значения, используемый для контекстной информации.

- %INPUT_NAME% — имя поля во входном потоке данных об угрозах. Оно должно быть определено в соответствии с форматом входного потока данных об угрозах:
  - Для входных потоков данных об угрозах в формате JSON значение %INPUT_NAME% должно содержать имя поля из входного потока данных об угрозах. Вложенные поля разделяются символом « / ».
  - Для входных потоков данных об угрозах в формате CSV значение %INPUT_NAME% должно содержать номер столбца.
  - Для входных потоков данных об угрозах в формате XML значение %INPUT_NAME% должно содержать путь к одному из вложенных элементов корневого элемента. Корневой элемент определяется в атрибуте `rootElement` элемента `Parsing`. Путь чувствителен к регистру.
  - Для входных потоков данных об угрозах STIX и MISP элемент `Parsing` не должен содержать правил парсинга.

В следующем примере демонстрируется синтаксис правила парсинга для входного формата JSON:

```
<Feed>
    ...
    <Parsing type="json">
        <Field type="url">URL</Field>
        <Field type="ip">IP</Field>
        <Field type="context">GEO</Field>
        <Field type="md5">files/md5</Field>
    </Parsing>
    ...
<Feed>
```

В следующем примере демонстрируется синтаксис правила парсинга для входного формата CSV:

```
<Feed>
    ...
    <Parsing type="csv" delimiter=";">
        <URL type="url">1</URL>
        <IP type="ip">2</IP>
        <GEO type="context">3</GEO>
        <MD5 type="md5">4</MD5>
    </Parsing>
    ...
<Feed>
```

В следующем примере демонстрируется синтаксис правила парсинга для входного формата XML:

```
<Feed>
    ...
    <Parsing type="xml" rootElement="Feeds/Example/Contents">
        <URL type="url">url</URL>
        <IP type="ip">ip</IP>
        <GEO type="context">context</GEO>
        <MD5 type="md5">md5_hash</MD5>
    </Parsing>
    ...
<Feed>
```

Правила парсинга для потоков данных об угрозах типа «электронная почта»

Чтобы задать правила парсинга для стороннего потока данных об угрозах, укажите следующие значения для атрибута `type`:

- `messageBody` – правила парсинга тела сообщения электронной почты.

  Это значение применимо, если в элементе `Path` включены протоколы POP3 или IMAP.

- `messageAttach` – правила парсинга вложения электронной почты.

  Это значение применимо, если в элементе `Path` включены протоколы POP3 или IMAP.

Парсинг тела сообщения (для потоков данных об угрозах типа «электронная почта»)

Feed Utility анализирует тело сообщения электронной почты, загруженного с почтового сервера, если в атрибуте `type` элемента `Parsing` задано значение `messageBody`.

Для парсинга тела сообщения используются регулярные выражения, указанные в элементе `Parsing`.

Для парсинга тела сообщения можно задать одно или несколько правил с регулярными выражениями.

Каждое правило имеет следующий вид:

```
<%FIELD_NAME% type="%FIELD_TYPE%">%REG_EXP%</%FIELD_NAME%>,
```

где:

%FIELD_NAME% определяет имя поля в выходном потоке данных об угрозах. Например, если %FIELD_NAME% — это «MD5», поле с этим значением в выходном потоке данных об угрозах также будет называться MD5.

%FIELD_TYPE% — тип индикатора.

%REG_EXP% — регулярное выражение.

Каждое регулярное выражение применяется ко всему телу сообщения.

Поток данных об угрозах формируется в соответствии с содержанием загруженных сообщений электронной почты. Формирование потока данных об угрозах удовлетворяет следующим условиям:

- Значения всех загруженных сообщений электронной почты отражаются в одном итоговом потоке данных об угрозах.

  Feed Utility сохраняет дату последнего обновления потока данных об угрозах. В случае обращения к почтовому серверу, парсинг применяется только к сообщениям электронной почты, полученным после предыдущего обновления потока данных об угрозах.

- Каждая запись итогового потока данных об угрозах содержит следующие поля:
  - `message_from` – адрес электронной почты отправителя сообщения.
  - `message_subject` – тема сообщения электронной почты.
  - `message_date` – дата получения сообщения электронной почты почтовым сервером.
- Каждая запись итогового потока данных об угрозах содержит только один индикатор, полученный в соответствии с одним регулярным выражением со значением атрибута `type`, отличным от CONTEXT.
- Каждое значение из сообщения электронной почты отражается в каждой записи итогового потока данных об угрозах, если это значение получено в соответствии с регулярным выражением, атрибут `type` которого имеет значение CONTEXT.

  Значения указываются в записях итогового потока данных об угрозах, которые содержат индикаторы (IP/HASH/URL) из того же сообщения электронной почты.

  Если для одного регулярного выражения получено более одного значения (с атрибутом type, имеющим значение CONTEXT), эти значения указываются в одной записи итогового потока данных об угрозах. Значения разделяются последовательностью символов «`;`».
- Поток данных об угрозах не будет содержать значения, соответствующие критериям правил, указанных в разделе `Excluded` (см. раздел «Исключенный элемент для потоков данных об угрозах типов „PDF“ и „электронная почта“» ниже).

Парсинг вложений сообщения (для потоков данных об угрозах типа «электронная почта»)

Feed Utility анализирует вложения сообщения электронной почты, загруженного с почтового сервера, если в атрибуте type элемента `Parsing` задано значение `messageAttach`.

Можно установить одно или несколько правил для типов вложенных файлов.

Каждое правило имеет следующий вид:

```
<Attach type="%ATTACH_TYPE%"></Attach>,
```

где:

%ATTACH_TYPE% — тип вложения.

%ATTACH_TYPE% может иметь следующие значения:

- `csv`
- `json`
- `xml`
- `stix`
- `stix2`
- `pdf`

Элемент `Attach` имеет хотя бы одно значение.

Можно задать одно или несколько правил с регулярными выражениями.

Каждое правило имеет следующий вид:

`<%FIELD_NAME% type="%FIELD_TYPE%">%REG_EXP%</%FIELD_NAME%>`,

где:

%FIELD_NAME% определяет имя поля в выходном потоке данных об угрозах. Например, если %FIELD_NAME% — это «MD5», поле с этим значением в выходном потоке данных об угрозах также будет называться MD5.

%REG_EXP% — регулярное выражение.

%FIELD_TYPE% — тип индикатора. Для элемента %FIELD_TYPE% в атрибуте `type` необходимо указать одно из следующих значений:

- ip
- md5
- sha256
- sha1
- url
- context

В следующем примере демонстрируется правило парсинга вложения сообщения:

```
<Attach type="pdf">
    <hash1 type="md5">([\da-fA-F]{32})</hash1>
    <hash2 type="sha1">([\da-fA-F]{40})</hash2>
</Attach>
```

Утилита Feed выполняет парсинг файлов со следующими расширениями:

Значение атрибута `type` элемента `Parsing`	Расширения файлов
csv	csv и txt
json	json
xml	xml
stix1	xml
stix2	json
pdf	pdf

Если правила парсинга заданы одновременно для stix1 и xml (или stix2 и json), Feed Utility выполняет следующие действия:

1. Пытается подвергнуть прикрепленный файл парсингу как stix (с расширением xml/json).
2. Если при парсинге не возникло ошибок и файл является корректным потоком данных об угрозах stix, парсинг этого файла в соответствии с правилами парсинга xml/json-вложений, указанными в настройках потока данных об угрозах, не выполняется.
3. Если во время парсинга произошла ошибка (файл не является корректным потоком данных об угрозах stix), этот файл подвергается парсингу в соответствии с правилами парсинга xml/json-вложений, указанными в настройках потока данных об угрозах.

Если в сообщении электронной почты содержится несколько вложений, информация из каждого вложения попадает в один итоговый поток данных об угрозах.

Поток данных об угрозах формируется в соответствии с содержанием загруженных сообщений электронной почты. Формирование потока данных об угрозах удовлетворяет следующим условиям:

- Значения всех загруженных вложений электронной почты отображаются в одном итоговом потоке данных об угрозах.

  Feed Utility сохраняет дату последнего обновления потока данных об угрозах. В случае обращения к почтовому серверу, парсинг применяется только к сообщениям электронной почты, полученным после предыдущего обновления потока данных об угрозах.

- Каждая запись итогового потока данных об угрозах содержит следующие поля:
  - `message_from` – адрес электронной почты отправителя сообщения.
  - `message_subject` – тема сообщения электронной почты.
  - `message_date` – дата получения сообщения электронной почты почтовым сервером.
  - `attach_name` – имя вложения.
- Каждая запись итогового потока данных об угрозах содержит только один индикатор, полученный в соответствии с одним регулярным выражением со значением атрибута `type`, отличным от CONTEXT.
- Каждое значение из вложения в сообщение электронной почты отражается в каждой записи итогового потока данных об угрозах, если это значение получено в соответствии с регулярным выражением, атрибут `type` которого имеет значение CONTEXT.

Значения указываются в записях итогового потока данных об угрозах, которые содержат индикаторы (IP/HASH/URL) из того же вложения электронной почты.

Если для одного регулярного выражения получено более одного значения (с атрибутом type, имеющим значение CONTEXT), эти значения указываются в одной записи итогового потока данных об угрозах. Значения разделяются последовательностью символов « ; ».

- Поток данных об угрозах не будет содержать значения, соответствующие критериям правил, указанных в разделе `Excluded` (см. раздел «Исключенный элемент для потоков данных об угрозах типов „PDF“ и „электронная почта“» ниже).

Исключенный элемент для потоков данных об угрозах типов «PDF» и «электронная почта»

Если значение `pdf, messageBody` или `messageAttach` указано в атрибуте `type` элемента `Parsing`, элемент `Feed` может содержать раздел `Excluded` и один или несколько вложенных элементов <Item/> с правилами исключения индикаторов для итогового потока данных об угрозах.

Раздел `Excluded` имеет следующий вид:

```
<Excluded>
    <Item>{RegExp}</Item>
    ...
</Excluded>
```

Где `{RegExp}` — регулярное выражение.

Элементы `Excluded` и `Item` не являются обязательными.

В следующем примере демонстрируются правила исключения:

```
<Excluded>
    <Item>(\w{3}\s+\d+\s+[\d\:]+)\s</Item>
    <Item>(https:\/\/badurl\.com)</Item>
</Excluded>
```

Коды возврата Feed Utility

После завершения работы Feed Utility она сообщает о своем успешном, частично успешном завершении работы или отказе с помощью кода возврата. Код возврата может иметь одно из значений, описанных ниже.

Значения кода возврата

Feed Utility возвращает следующие значения:

- `0`

  Успех.

  Feed Utility успешно выполнила все действия.

  Например, если Feed Utility настроена на загрузку и обработку двух потоков данных об угрозах, этот код возврата означает, что оба потока данных об угрозах были успешно загружены и обработаны.

- `1`

Отказ.

Все действия, выполненные программой Feed Utility, завершились отказом или их не удалось выполнить.

Например, если Feed Utility настроена на загрузку и обработку двух потоков данных об угрозах, этот код может означать, что какие-либо потоки данных об угрозах не были загружены из-за сетевой ошибки.

Это значение возвращается, если из-за правил фильтрации ни в один из обработанных файлов потоков данных об угрозах не была выполнена запись.

- `2`

  Частичный успех.

  Feed Utility успешно выполнила некоторые из действий.

  Например, если Feed Utility настроена на загрузку и обработку двух потоков данных об угрозах, этот код возвращается, если был успешно загружен и обработан только один из потоков данных об угрозах.

  Это значение также возвращается, если из-за правил фильтрации в один из обработанных файлов потоков данных об угрозах не была выполнена запись.

- `3`

  Нечего загружать.

  Это значение возвращается в следующих случаях:

  - Потоки данных об угрозах не были загружены и обработаны в Feed Utility (когда атрибут `enabled` в конфигурационном файле Feed Utility имеет значение `false`)
  - Потоки данных об угрозах не были обновлены, поскольку уже имеется актуальная версия потоков данных об угрозах

Использование Kaspersky CyberTrace в режиме высокой доступности

В этом разделе описывается порядок настройки Kaspersky CyberTrace для работы в режиме высокой доступности, порядок развертывания Balancer и управления им из командной строки или с помощью скрипта.

О Balancer

Balancer — это один из компонентов Kaspersky CyberTrace. Он работает как служба и позволяет использовать Kaspersky CyberTrace в режиме высокой доступности.

Режим высокой доступности используется, когда в одной локальной сети развернуто несколько экземпляров Kaspersky CyberTrace.

При установке HTTPS-соединений с экземплярами Kaspersky CyberTrace служба Balancer проверяет HTTPS-сертификаты на соответствие эталонным сертификатам.

В режиме высокой доступности поддерживаются следующие функции Kaspersky CyberTrace:

- Сопоставление входящих событий с потоками данных об угрозах и источниками данных об угрозах.
- REST API Kaspersky CyberTrace.

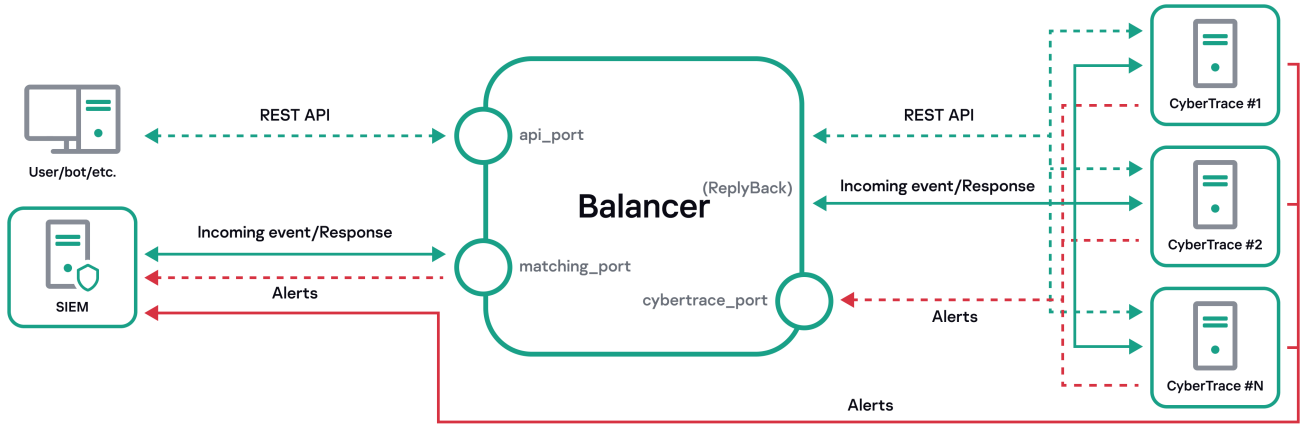
  Можно использовать следующие запросы REST API:

  - POST lookup
  - GET suppliers
  - GET suppliers/{supplier}
- Экспорт индикаторов в CSV

Такая схема развертывания позволяет добиться следующего:

1. Снижение нагрузки на каждый экземпляр Kaspersky CyberTrace.
2. Обеспечение отказоустойчивости сопоставления входящих событий, обработки запросов REST API и экспорта индикаторов в случае сбоя одного экземпляра.

Balancer направляет входящие события и запросы REST API на экземпляры Kaspersky CyberTrace, где выполняется процесс сопоставления. Затем Balancer получает результаты сопоставления, используя режим ReplyBack mode.



Использование Kaspersky CyberTrace в режиме высокой доступности

Требования и ограничения

Правильная работа Kaspersky CyberTrace в режиме высокой доступности требует выполнения следующих условий:

1. Все экземпляры Kaspersky CyberTrace должны иметь идентичные настройки.
2. Добавленные вручную поля контекста, а также индикаторы в источниках данных об угрозах FalsePositive и InternalTI, добавленные с помощью веб-интерфейса Kaspersky CyberTrace или REST API, должны быть идентичными во всех экземплярах Kaspersky CyberTrace.

3. Все экземпляры Kaspersky CyberTrace должны иметь задачи экспорта индикаторов с идентичными именами и правилами фильтрации.

4. На всех экземплярах Kaspersky CyberTrace и Balancer должен действовать один и тот же уровень лицензирования.

Ответственность за выполнение вышеуказанных условий возлагается на администратора системы. Если эти условия не будут выполнены, корректная работа Kaspersky CyberTrace в режиме высокой доступности не гарантируется.

Использование Kaspersky CyberTrace в режиме высокой доступности связано со следующими ограничениями:

1. Поскольку между экземплярами Kaspersky CyberTrace не поддерживается синхронизация, индикаторы в их базах данных могут в каждый конкретный момент времени немного различаться.

2. Режим высокой доступности поддерживает только ограниченное подмножество запросов REST API. Balancer предварительно настроен на использование всех поддерживаемых типов запросов (более подробные сведения приведены в описании элемента `AllowedRequests` в разделе Настройка Balancer).

3. На одном конкретном экземпляре Kaspersky CyberTrace невозможно просмотреть статистику обнаруженных киберугроз по всем экземплярам.

4. Если один из экземпляров Kaspersky CyberTrace становится недоступным после того, как на этот экземпляр было отправлено событие или запрос REST API, результат сопоставления событий или обработки запроса будет утрачен.

5. Информационные события не отправляются в SIEM.

Развертывание Balancer

Файлы, необходимые для запуска Balancer, входят в комплект поставки. Balancer может развертываться как на сервере, на котором установлен экземпляр Kaspersky CyberTrace, так и на сервере без Kaspersky CyberTrace.

Развертывание на сервере с экземпляром Kaspersky CyberTrace

Чтобы развернуть Balancer на сервере с установленным экземпляром Kaspersky CyberTrace, выполните следующие действия:

1. Настройте Balancer.

2. Настройте экземпляры Kaspersky CyberTrace.

3. Запустите Balancer.

Развертывание на сервере без экземпляра Kaspersky CyberTrace

Чтобы развернуть Balancer на сервере без установленного экземпляра Kaspersky CyberTrace, выполните следующие действия:

1. Скопируйте файлы, перечисленные в таблице ниже, из каталога установки Kaspersky CyberTrace на другой сервер.

   Для каталога, в который копируются эти файлы, должны быть настроены строгие правила Списка контроля доступа. А именно, доступ к каталогу, его подкаталогам и содержащимся в них файлам должен иметь только администратор (в Windows) или root (в Linux).
   Кроме того, после копирования или редактирования этих файлов (например, после редактирования конфигурационного файла) необходимо убедиться, что правила Списка контроля доступа, примененные к каталогу и его содержимому, остаются строгими.

   Файлы, необходимые для установки Balancer на сервере без Kaspersky CyberTrace

Имя и расположение (Windows)	Имя и расположение (Linux)	Описание
`bin\kl_balancer.exe`	`bin/kl_balancer`	Бинарный файл Balancer.
`bin\kl_balancer.conf`	`bin/kl_balancer.conf`	Конфигурационный файл Balancer. Конфигурационный файл должен находиться в том же каталоге, что и бинарный файл Balancer.
`bin\kl_balancer_log.conf`	`bin/kl_balancer_log.conf`	Конфигурационный файл журнала Balancer. Конфигурационный файл должен находиться в том же каталоге, что и бинарный файл Balancer.
`httpsrv\kl_feed_service_cert.pem`	`httpsrv/kl_feed_service_cert.pem`	Сертификат в формате PEM для HTTPS-соединений.
`httpsrv\kl_feed_service_private.pem`	`httpsrv/kl_feed_service_private.pem`	Закрытый ключ в формате PEM для HTTPS-соединений.
`httpsrv\lic\*.key`	`httpsrv/lic/*.key`	Файл лицензионного ключа

2. В файле `kl_balancer.conf` необходимо прописать пути к следующим файлам:

   - `kl_feed_service_cert.pem`
   - `kl_feed_service_private.pem`
   - Файл лицензионного ключа

   Balancer и все экземпляры Kaspersky CyberTrace должны работать на одном и том же уровне лицензирования. Если лицензионный ключ не предоставлен, Balancer будет работать на уровне лицензирования Community Edition и обрабатывать не более 250 событий в секунду.

3. Настройте Balancer.

4. Настройте экземпляры Kaspersky CyberTrace.

5. Запустите Balancer.

Проверка HTTPS-сертификатов

При установке HTTPS-соединения с экземплярами Kaspersky CyberTrace служба Balancer проверяет, соответствует ли сертификат, полученный от Kaspersky CyberTrace, эталонному сертификату, расположенному в каталоге, указанном в качестве значения параметра `CertDirPath` файла конфигурации `kl_balancer.conf`.

> Проверка сертификатов возможна только в Rest API, поскольку только Rest API работает с https. Этот раздел не применим к обнаружению.

Если эталонный сертификат экземпляра Kaspersky CyberTrace недоступен в каталоге или каталога не существует, Balancer выполняет следующие действия:

1. Сохраняет сертификат, полученный от Kaspersky CyberTrace, в файл `%CERT_PATH%/%INSTANCE%_%CT_PORT%.pem`, где:

   - `CERT_PATH` – каталог, указанный в качестве значения параметра `CertDirPath` конфигурационного файла `kl_balancer.conf`.

   - `INSTANCE` – имя хоста/значение IP-адреса, указанное в качестве значения элемента `Instances` > `Instance` для определенного экземпляра Kaspersky CyberTrace.

   - `CT_PORT` – значение порта, указанное в качестве значения атрибута `matching_port` элемента `Instances` > `Instance` для определенного экземпляра Kaspersky CyberTrace.

2. Продолжает устанавливать HTTPS-соединение с использованием полученного сертификата.

Если сертификат Kaspersky CyberTrace не соответствует эталонному сертификату, Balancer выполняет следующие действия:

1. Прекращает установку HTTPS-соединения с экземпляром Kaspersky CyberTrace.

2. Возвращает код статуса 500 со следующей информацией об ошибке:

   - IP-адрес или имя хоста экземпляра Kaspersky CyberTrace.

   - Номер порта экземпляра Kaspersky CyberTrace.

   - Описание проблемы: HTTPS-соединение с экземпляром Kaspersky CyberTrace не установлено, поскольку сертификат сервера не соответствует ожидаемому.

> Если имя хоста, IP-адрес или порт экземпляра Kaspersky CyberTrace, используемого при развертывании в режиме высокой доступности, изменены, эталонный сертификат экземпляра будет сохранен повторно. Старый сертификат не удаляется автоматически. За удаление неиспользованных сертификатов отвечает администратор Kaspersky CyberTrace.

Изменение сертификата Kaspersky CyberTrace

При изменении сертификата на стороне Kaspersky CyberTrace требуется вручную изменить сертификат на стороне Balancer.

Чтобы изменить сертификат Kaspersky CyberTrace, выполните следующие действия:

1. Остановите службу экземпляра Kaspersky CyberTrace.

   `sc stop cybertrace` (в Windows)

   `systemctl stop cybertrace.service` (в Linux)

2. Измените сертификат экземпляра Kaspersky CyberTrace.

3. Запустите службу экземпляра Kaspersky CyberTrace.

   `sc start cybertrace` (в Windows)

   `systemctl start cybertrace.service` (в Linux)

4. Остановите службу Balancer.

   `sc stop KasperskyBalancerService` (в Windows)

   `systemctl stop cybertrace_balancer.service` (в Linux)

5. На стороне Balancer измените сертификат для экземпляра Kaspersky CyberTrace.

   На стороне Kaspersky CyberTrace скопируйте файл `httpsrv\kl_feed_service_cert.pem` и вставьте его в каталог `%CERT_PATH%` на стороне Balancer, а затем переименуйте в `%INSTANCE%_%CT_PORT%.pem`.

6. Запустите службу Balancer.

   `sc start KasperskyBalancerService` (в Windows)

   `systemctl start cybertrace_balancer.service` (в Linux)

Более подробные сведения об изменении сертификатов приведены в разделе Генерация SSL-сертификатов для веб-интерфейса Kaspersky CyberTrace.

Проверка параметров сертификата

Чтобы проверить параметры сертификата выбранного экземпляра Kaspersky CyberTrace:

1. Остановите службу Balancer.

   `sc stop KasperskyBalancerService` (в Windows)

   `systemctl stop cybertrace_balancer.service` (в Linux)

2. Для всех экземпляров Kaspersky CyberTrace, кроме выбранного, укажите `enabled = "false"` в разделе `Instances` конфигурационного файла `kl_balancer.conf`.

3. Запустите службу Balancer.

   `sc start KasperskyBalancerService` (в Windows)

   `systemctl start cybertrace_balancer.service` (в Linux)

4. Отправьте любой запрос, указанный в разделе AllowedRequests (например, `GET/api/v.1.1/suppliers`), на порт Balancer (указанный в качестве значения параметра `api_port`).

5. Убедитесь, что получен ответ со статусом 200, а также список используемых источников.

6. Остановите службу Balancer.

   `sc stop KasperskyBalancerService` (в Windows)

   `systemctl stop cybertrace_balancer.service` (в Linux)

7. Для всех экземпляров Kaspersky CyberTrace из шага 2 укажите `enabled = "true"` в разделе `Instances` конфигурационного файла `kl_balancer.conf`.

8. Запустите службу Balancer.

   `sc start KasperskyBalancerService` (в Windows)

   `systemctl start cybertrace_balancer.service` (в Linux)

Настройка экземпляров Kaspersky CyberTrace

В этом разделе описывается порядок настройки экземпляров Kaspersky CyberTrace для использования в режиме высокой доступности.

Для использования Kaspersky CyberTrace в режиме высокой доступности необходимо настроить все экземпляры Kaspersky CyberTrace следующим образом:

1. Импортируйте один и тот же сертификат для потоков данных об угрозах Kaspersky Threat Data Feeds.

2. Включите одни и те же потоки данных об угрозах Kaspersky Threat Data Feeds.

3. Включите одни и те же потоки данных об угрозах OSINT, а также в случае необходимости добавьте и настройте идентичные пользовательские и сторонние потоки данных об угрозах.

   > Поля контекста, добавленные вручную, а также индикаторы в источниках данных об угрозах FalsePositive и InternalTI, добавленные с помощью веб-интерфейса Kaspersky CyberTrace или REST API, должны быть идентичными во всех экземплярах Kaspersky CyberTrace.

4. Добавьте один и тот же лицензионный ключ или используйте режим Community Edition для всех экземпляров.

5. Добавьте задачи экспорта индикаторов с одинаковыми именами и правилами фильтрации.

6. Укажите следующее идентичное регулярное выражение для сопоставления входящих событий от Balancer:

   Регулярное выражение для сопоставления входящих событий от Balancer

Тип индикатора	Имя правила	Регулярное выражение
CONTEXT	REQ	^(\d+)\s

   Для регулярного выражения можно использовать любое разрешенное имя, однако важно убедиться, что то же имя регулярного выражения используется в шагах настройки ниже.

   Можно указать регулярное выражение в источнике событий по умолчанию или создать новое.

7. Задайте идентичные параметры формата событий для оповещений об обнаружении индикаторов компрометации и служебных оповещений.

   Каждое событие должно начинаться со значения, которое было извлечено из входящего события регулярным выражением `REQ`. Например: `%REQ% category=%Category% %RecordContext%`.

8. Настройте формат оповещений, генерируемых Kaspersky CyberTrace в ответ на каждое полученное событие:

   a. Остановите Kaspersky CyberTrace Service следующей командой:

   - `systemctl stop cybertrace.service` (в Linux)
   - `sc stop cybertrace` (в Windows)

   b. В элементе `OutputSettings → FinishedEventFormat` конфигурационного файла службы Kaspersky CyberTrace задайте следующий формат оповещений:

   ```
   <FinishedEventFormat enabled="true">%REQ% LookupFinished</FinishedEventFormat>
   ```

   Эти оповещения предназначены только для внутреннего пользования. Они не отправляются в SIEM.

   c. Сохраните конфигурационный файл.

   d. Запустите Kaspersky CyberTrace Service:

   - `systemctl start cybertrace.service` (в Linux)
   - `sc start cybertrace` (в Windows)

Если требуется, можно также задать настройки соединения для отправки служебных оповещений в Balancer в разделе **Служебные оповещения** на вкладке **Параметры** → **Служба**. Используйте следующие параметры из файла `kl_balancer.conf`:

- IP-адрес, указанный в элементе `Balancer`
- Порт, указанный в параметре `cybertrace_port` элемента `Balancer`

Служебные оповещения можно отправлять непосредственно в SIEM.

Параметры отправки оповещений об обнаружении индикаторов компрометации в режиме высокой доступности не используются, поскольку Balancer получает результаты сопоставления событий в режиме ReplyBack mode.

Лицензирование

Balancer использует тот же уровень лицензирования, что и Kaspersky CyberTrace, и подпадает под ограничение на количество событий в секунду. Подробные сведения о лицензировании приведены в разделе О лицензировании.

При развертывании Balancer на сервере без Kaspersky CyberTrace скопируйте файл лицензионного ключа, если он имеется, из `каталога httpsrv\lic\` (в Windows) или `httpsrv/lic/` (в Linux), а затем укажите соответствующий локальный путь в конфигурационном файле `kl_balancer.conf`.

Balancer и все экземпляры Kaspersky CyberTrace должны работать на одном и том же уровне лицензирования. Если лицензионный ключ не предоставлен, Balancer будет работать на уровне лицензирования Community Edition и обрабатывать не более 250 событий в секунду.

Настройка Balancer

Параметры Balancer задаются в конфигурационном файле `kl_balancer.conf`, входящем в комплект поставки. `kl_balancer.conf` представляет собой XML-файл, содержащий параметры, описанные в таблице ниже.

Параметры конфигурационного файла

Параметр	Описание
`Balancer`	Задает адрес для подключения к Balancer. Значение может быть IPv4-адресом, IPv6-адресом или именем хоста. Необходимо указать следующие параметры: • `matching_port` — порт, на котором Balancer принимает входящие события. Диапазон значений этого параметра: от `1` до `65535`. Этот параметр является обязательным. • `api_port` — порт, на котором Balancer принимает запросы API. Диапазон значений этого параметра: от `1` до `65535`. Этот параметр является обязательным. • `cybertrace_port` — порт, на котором Balancer получает системные оповещения от экземпляров Kaspersky CyberTrace. Диапазон значений этого параметра: от `1` до `65535`. Этот параметр является обязательным. • `scanners_count` — максимальное количество одновременных подключений. Диапазон значений этого параметра: от `1` до `100`. Этот параметр является обязательным. Этот элемент является обязательным. В конфигурационном файле может быть только один элемент `Balancer`.
`EventDelimiter`	Регулярное выражение, определяющее разделитель для событий. Этот элемент не является обязательным. Если событие содержит символы новой строки (`\n`), разбиение такого события произойдет как по символу, заданному в этом параметре, так и по символу новой строки.
`SSLCertificatePath`	Путь к сертификату в формате PEM для HTTPS-соединений. Этот элемент может содержать абсолютный или относительный путь. Если указан относительный путь, он отсчитывается относительно бинарного файла Balancer. Этот параметр является необязательным. По умолчанию задано следующее значение: • В системах Windows: `..\httpsrv\kl_feed_service_cert.pem`. • В системах Linux: `../httpsrv/kl_feed_service_cert.pem`. Значение этого элемента следует изменить, если Balancer развернут на сервере без Kaspersky CyberTrace.

Параметр	Описание
`SSLPrivateKeyPath`	Путь к закрытому ключу в формате PEM для HTTPS-соединений. Этот элемент может содержать абсолютный или относительный путь. Если указан относительный путь, он отсчитывается относительно бинарного файла Balancer. Этот параметр является необязательным. По умолчанию задано следующее значение: • В системах Windows: `..\httpsrv\kl_feed_service_private.pem`. • В системах Linux: `../httpsrv/kl_feed_service_private.pem`. Значение этого элемента следует изменить, если Balancer развернут на сервере без Kaspersky CyberTrace.
`LicenseDirPath`	Путь к каталогу с файлом лицензионного ключа. Этот элемент может содержать абсолютный или относительный путь. Если указан относительный путь, он отсчитывается относительно бинарного файла Balancer. Этот параметр является необязательным. По умолчанию задано следующее значение: • В системах Windows: `..\httpsrv\lic`. • В системах Linux: `../httpsrv/lic`. Значение этого элемента следует изменить, если Balancer развернут на сервере без Kaspersky CyberTrace.
`CertDirPath`	Путь к каталогу с сертификатами Kaspersky CyberTrace. Этот элемент может содержать абсолютный или относительный путь. Если указан относительный путь, он отсчитывается относительно исполняемого файла Balancer. Этот параметр является обязательным. По умолчанию задано следующее значение: `..\etc\certs`
`OutputSettings`	Задает адрес для отправки результатов сопоставления входящих событий. Значение может быть IPv4-адресом, IPv6-адресом или именем хоста. Можно указать следующий параметр: • `port` — порт, на который Balancer отправляет результаты сопоставления входящих событий. Диапазон значений этого параметра: от `1` до `65535`. Этот параметр является обязательным. Этот элемент является обязательным.
`FinishedEventFormat`	Указывает на необходимость отправки сообщения о завершении сопоставления и формат этого сообщения. Этот элемент может содержать строку, которая должна соответствовать следующим требованиям: • длина от 1 до 2048 символов; • только символы ASCII. Этот элемент обладает следующими атрибутами: • enabled Этот атрибут может принимать значения `true` или `false`. По умолчанию задано значение `false`. По умолчанию для этого элемента задано значение `LookupFinished`. Этот элемент не является обязательным. Пример формата: `<FinishedEventFormat enabled="false">LookupFinished</FinishedEventFormat>`

Параметр	Описание
`Instances`	Раздел, содержащий элементы с параметрами экземпляров Kaspersky CyberTrace. Для раздела можно задать следующие параметры: • `update_seconds` — интервал времени в секундах между попытками подключения к недоступным экземплярам Kaspersky CyberTrace. Этот параметр является обязательным. Диапазон значений этого параметра: от `1` до `3600`. • `matching_timeout_seconds` — время ожидания ответа от экземпляра Kaspersky CyberTrace с результатом сопоставления входящего события, в секундах. Этот параметр является обязательным. Диапазон значений этого параметра: от `1` до `3600`. • `api_timeout_seconds` — время ожидания ответа от экземпляра Kaspersky CyberTrace на запрос REST API в секундах. Этот параметр является обязательным. Диапазон значений этого параметра: от `1` до `3600`. Этот элемент является обязательным.
`Instances/Instance`	Элемент с параметрами подключения к экземпляру Kaspersky CyberTrace. Значение может быть адресом IPv4 или IPv6. Этот элемент является обязательным. Можно указать следующие параметры: • `enabled` — задает состояние экземпляра Kaspersky CyberTrace. Этот параметр является обязательным. Этот параметр может принимать значения `true` или `false`. • `matching_port` — порт, на котором экземпляр Kaspersky CyberTrace принимает входящие события. Значение этого параметра должно соответствовать значению элемента *InputSettings > ConnectionString* в конфигурационном файле экземпляра Kaspersky CyberTrace. Этот параметр является обязательным. Диапазон значений этого параметра: от `1` до `65535`. • `api_port` — порт, на котором экземпляр Kaspersky CyberTrace принимает запросы REST API. Значение этого параметра должно соответствовать значению элемента *HTTPServer > ConnectionString* element in the configuration file of the Kaspersky CyberTrace instance. Этот параметр является обязательным. Диапазон значений этого параметра: от `1` до `65535`. • `scanners_count` — максимальное количество одновременных подключений, разрешенных для экземпляра Kaspersky CyberTrace. Этот параметр является обязательным. Диапазон значений этого параметра: от `1` до `100`. Значение параметра `scanners_count` для экземпляра Kaspersky CyberTrace не должно превышать значение (меньше 1) параметра `ScannersCount`, указанного в конфигурационном файле данного экземпляра Kaspersky CyberTrace. Этот элемент является обязательным.
`AllowedRequests`	Раздел, содержащий элементы с параметрами разрешенных запросов REST API к экземплярам Kaspersky CyberTrace. Этот элемент является обязательным.

Параметр	Описание
`AllowedRequests/AllowedRequest`	Элемент, содержащий параметры отдельного разрешенного запроса REST API к экземплярам Kaspersky CyberTrace. Этот элемент не является обязательным. Этот элемент может содержать строку длиной от 1 до 2048 символов, содержащую только символы ASCII. Значение этого элемента может содержать подстановочный знак «*», обозначающий ноль или более любых символов. Можно указать следующий параметр: • `method` — метод запроса. В качестве значения этого параметра можно использовать `GET`, `POST`, `PUT` или `DELETE`. Этот параметр является обязательным. Значение этого параметра нечувствительно к регистру. По умолчанию файл `kl_balancer.conf` содержит все элементы `AllowedRequest`, необходимые для работы REST API Kaspersky CyberTrace.

Конфигурационный файл, используемый по умолчанию.

По умолчанию файл `kl_balancer.conf` содержит следующие параметры:

```
<Settings>
    <Balancer matching_port="9998" api_port="9997" cybertrace_port="9996" scanners_count="9">127.0.0.1</Balancer>
    <SSLCertificatePath>..\httpsrv\kl_feed_service_cert.pem</SSLCertificatePath>
    <SSLPrivateKeyPath>..\httpsrv\kl_feed_service_private.pem</SSLPrivateKeyPath>
    <LicenseDirPath>..\httpsrv\lic</LicenseDirPath>
    <OutputSettings port="514">127.0.0.1</OutputSettings>
    <Instances update_seconds="60" matching_timeout_seconds="5" api_timeout_seconds="30">
        <Instance enabled="true" matching_port="9999" api_port="443" scanners_count="8">127.0.0.1</Instance>
    </Instances>
    <AllowedRequests>
        <AllowedRequest method="GET">/api/1.2/suppliers</AllowedRequest>
        <AllowedRequest method="GET">/api/1.2/suppliers/*</AllowedRequest>
        <AllowedRequest method="POST">/api/1.2/lookup</AllowedRequest>
        <AllowedRequest method="GET">/api/1.2/tags</AllowedRequest>
        <AllowedRequest method="GET">/ioc_exports/*</AllowedRequest>
    </AllowedRequests>
</Settings>
```

Вышеприведенный конфигурационный файл по умолчанию входит в состав комплекта поставки для систем Windows. Конфигурационный файл по умолчанию для систем Linux имеет то же содержимое, за исключением формата локальных путей в значениях параметров `SSLCertificatePath`, `SSLPrivateKeyPath` и `LicenseDirPath`, где обратная косая черта («\») заменяется прямой («/»).

Управление Balancer

В этом разделе описывается порядок управления Balancer.

Управление Balancer посредством systemd (Linux)

Для управления Balancer можно использовать systemd.

Все стандартные команды systemd могут применяться для управления Balancer.

Добавление Balancer в systemd

Чтобы добавить Balancer в systemd, выполните следующие действия:

1. Скопируйте файл `cybertrace_balancer.service` из каталога `etc/systemd/system/` в комплекте поставки в каталог `/etc/systemd/system` системы.
2. Выполните следующую команду:

```
systemctl daemon-reload

systemctl enable cybertrace_balancer.service
```

Проверка статуса Balancer

Для проверки статуса Balancer используется следующая команда:

```
systemctl status cybertrace_balancer.service
```

Запуск, остановка и перезапуск Balancer.

Для запуска Balancer используется следующая команда:

```
systemctl start cybertrace_balancer.service
```

Для остановки Balancer используется следующая команда:

```
systemctl stop cybertrace_balancer.service
```

Для перезапуска Balancer используется следующая команда:

```
systemctl restart cybertrace_balancer.service
```

Удаление Balancer из systemd

Чтобы удалить Balancer из systemd, выполните следующие действия:

1. Выполните следующую команду:

   ```
   systemctl disable cybertrace_balancer.service
   ```

2. Удалите файл `/etc/systemd/system/cybertrace_balancer.service`.

3. Выполните следующую команду:

   ```
   systemctl daemon-reload
   ```

Управление Balancer посредством Диспетчера управления службами (Windows)

В системах Windows управление Balancer осуществляется с помощью Диспетчера управления службами (SCM).

Для управления Balancer используются следующие команды:

- `sc start KasperskyBalancerService`
- `sc stop KasperskyBalancerService`
- `sc query KasperskyBalancerService`

Подробные сведения приведены в разделе Управление Kaspersky CyberTrace Service с помощью SCM (Windows).

Регистрация Balancer в качестве службы Windows

Перед использованием Balancer необходимо зарегистрировать его как службу Windows.

Чтобы зарегистрировать Balancer в качестве службы Windows, выполните следующие действия:

Выполните следующую команду:

```
kl_balancer.exe --reg
```

Удаление службы Balancer

Чтобы удалить службу Balancer, выполните следующие действия:

Выполните следующую команду:

```
kl_balancer.exe --del
```

Журнал Balancer

Balancer использует параметры ведения журнала, заданные в файле `kl_balancer_log.conf`.

При развертывании Balancer на сервере без Kaspersky CyberTrace скопируйте `kl_balancer_log.conf` из каталога `bin` в тот же каталог, что и бинарный файл Balancer.

Формат имен файлов журналов

Balancer записывает сообщения в файлы с именами `kl_balancer-<pid>-<date_time>.log`.

Содержимое файла журнала

Если используется уровень ведения журнала `err`, Balancer записывает в журнал следующую информацию:

- Ошибки, возникшие при инициализации Balancer.
- Ошибки, возникшие при установлении соединений с экземплярами Kaspersky CyberTrace.
- Ошибки, возникшие при установлении соединения с клиентом REST API.
- Ошибки, возникшие при получении результатов сопоставления событий.
- Служебные оповещения от Kaspersky CyberTrace.

Если используется уровень ведения журнала `inf`, Balancer записывает в журнал следующую информацию:

- Версия Balancer, версия ОС и PID процесса Balancer.
- Информация, записываемая на уровне ведения журнала `err`.
- Установление или закрытие соединений с экземплярами Kaspersky CyberTrace.
- Установление или закрытие соединения с клиентом REST API.
- Обмен запросами и ответами с экземплярами Kaspersky CyberTrace.

- Обмен запросами и ответами с клиентом REST API.
- Переключение Balancer в режим «ReplyBack mode».
- Переключение Balancer на работу в пределах лимита EPS.
- Переключение Balancer на работу без лимита EPS.
- Среднее значение EPS за час.
- Изменения уровня лицензирования Kaspersky CyberTrace.

Если используется уровень ведения журнала `dbg`, Balancer записывает в журнал следующую информацию:

- Информация, записываемая на уровне ведения журнала `inf`.
- Значения параметров конфигурационного файла Balancer.

  Эта информация записывается в журнал при инициализации Balancer.
- Входящие события, обрабатываемые Balancer.

> Если в каталоге бинарного файла Balancer отсутствует файл `kl_balancer_log.conf`, Balancer не ведет журнал.

Использование Password Utility

Password Utility представляет собой инструмент сброса пароля учетной записи `admin`.

> Для входа в Kaspersky CyberTrace следует использовать предустановленные имя пользователя и пароль.

Расположение

Password Utility расположена по следующему пути:

- В системах Windows:

  `%service_dir%\tools\kl_access_util.exe`
- В системах Linux:

  `%service_dir%/tools/kl_access_util`

Здесь `%service_dir%` — это каталог установки Kaspersky CyberTrace.

Синтаксис

Для вызова Password Utility используется следующий синтаксис:

- В системах Windows:

  ```
  kl_access_util.exe [[--help|-h] | [--reset_default_user|-r] | [--version|-v]]
  ```

- В системах Linux:

  ```
  ./kl_access_util [[--help|-h] | [--reset_default_user|-r] | [--version|-v]]
  ```

Параметры

Параметры командной строки описаны в следующей таблице.

Параметры командной строки kl_access_util

Параметр	Описание
`--help` `-h`	Вывод на экран сообщения о порядке использования. Если указан этот параметр, все остальные параметры игнорируются.
`--reset_default_user` `-r`	Пароль учетной записи `admin` сбрасывается на заданный по умолчанию, затем все остальные учетные записи пользователей удаляются. Если учетная запись `admin` отсутствует, утилита создает ее.
`--version` `-v`	Вывод информации о версии.

Выбор оптимальных потоков данных об угрозах для определенных условий работы

Выбор оптимальных потоков данных об угрозах для определенных условий работы позволяет снизить нагрузку на систему. Веб-интерфейс Kaspersky CyberTrace позволяет сравнивать используемые потоки данных об угрозах, а также находить и отключать потоки данных об угрозах, использование которых может быть нецелесообразно в конкретных условиях эксплуатации.

Эффективные потоки данных об угрозах

Ниже приведены характеристики, помогающие распознать эффективные потоки данных об угрозах:

- Большое количество обнаруженных киберугроз
- Частые обновления

  Потоки данных, которые часто обновляются, содержат более достоверную информацию.

Неэффективные потоки данных об угрозах

Ниже приведены характеристики, помогающие распознать неэффективные потоки данных об угрозах:

- Многие из корректно обнаруженных объектов не представляют опасности в конкретных условиях работы.
- Многие из обнаруженных киберугроз являются ложными срабатываниями.
- Поток данных об угрозах содержит много записей, но производит небольшое количество обнаруженных киберугроз.

Сравнение потоков данных об угрозах

Чтобы выбрать лучшие потоки данных об угрозах для решения, можно оценить их по следующим критериям:

- Количество обнаруженных киберугроз
- Количество ложных срабатываний
- Количество записей
- Частота обновления

Сравнить различные характеристики потоков данных об угрозах можно в веб-интерфейсе Kaspersky CyberTrace.

- Чтобы сравнить количество обнаруженных киберугроз, количество ложных срабатываний и количество записей в разных потоках данных об угрозах, обратитесь к таблицам и диаграммам на виджете **Статистика по потокам индикаторов** на странице **Информационная панель** веб-интерфейса Kaspersky CyberTrace.
- Чтобы узнать, какие типы индикаторов чаще всего обнаруживаются, обратитесь к таблицам и диаграммам в виджете **Статистика сопоставлений**.

Просмотр полей потока данных об угрозах

Чтобы решить, целесообразно ли использовать тот или иной поток данных об угрозах, можно просмотреть список его доступных полей. Просмотреть список полей конкретного потока данных об угрозах можно в веб-интерфейсе Kaspersky CyberTrace.

Чтобы просмотреть список полей определенного потока данных об угрозах, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace откройте страницу **Параметры → Потоки данных**.
2. В столбце **Действия** нажмите ссылку для потока данных, чтобы просмотреть его свойства.

Обновление и управление установкой

В этом разделе описывается порядок управления установленным ПО Kaspersky CyberTrace.

Управление установкой в ОС Linux

Для управления установкой Kaspersky CyberTrace из пакета RPM или DEB можно использовать скрипт установки.

Скрипт установщика обеспечивает следующие возможности:

- Установка Kaspersky CyberTrace
- Обновление Kaspersky CyberTrace
- Удаление Kaspersky CyberTrace
- Изменение конфигурации Kaspersky CyberTrace

Параметры командной строки скрипта установки

В командной строке сценария установки используется следующий синтаксис:

```
run.sh [команда]
```

Поддерживаются следующие команды:

- `help`

  Отображение справочного сообщения и завершение работы.

- `install`

  Установка Kaspersky CyberTrace.

Скрипт установки устанавливает пакет ПО и запускает бинарный файл конфигуратора. Бинарный файл конфигуратора выполняет интерактивную настройку Kaspersky CyberTrace Service, Feed Utility и Log Scanner.

- `upgrade`

  Обновление предыдущей версии Kaspersky CyberTrace.

  Скрипт установки обновляет программный пакет, копирует настройки из предыдущей версии Kaspersky CyberTrace Service, Feed Utility и Log Scanner, а затем запускает бинарный файл конфигуратора.

- `remove`

  Удаление (деинсталляция) Kaspersky CyberTrace.

  Скрипт установки удаляет программный пакет, удаляет каталог `/opt/kaspersky/ktfs`, удаляет Kaspersky CyberTrace Service из списка системных служб и удаляет записи crontab, относящиеся к Kaspersky CyberTrace Service.

- `change`

  Изменение конфигурации Kaspersky CyberTrace.

  Скрипт установки запускает бинарный файл конфигуратора.

  С помощью этой команды можно генерировать SSL-сертификаты для веб-интерфейса Kaspersky CyberTrace.

Примеры

Следующая команда устанавливает Kaspersky CyberTrace.

```
./run.sh install
```

Следующая команда обновляет Kaspersky CyberTrace.

```
./run.sh upgrade
```

Следующая команда удаляет Kaspersky CyberTrace.

```
./run.sh remove
```

Следующая команда изменяет конфигурацию Kaspersky CyberTrace.

```
./run.sh change
```

Действия в случае ошибки при установке

Во время установки после остановки Kaspersky CyberTrace Service конфигурационные файлы и некоторые другие файлы перемещаются во временный каталог /opt/kaspersky_cybertrace_tmp. Если во время установки возникают ошибки, перемещенные файлы остаются в этом временном каталоге.

Файл журнала обновления находится в каталоге `/temp` или в каталоге, указанном в переменной среды `$TEMP`, если переменная `$TEMP` определена.

Если в ходе автоматической установки возникла ошибка, обратитесь по адресу intelligence@kaspersky.com для получения дополнительной информации о способах решения проблемы.

Управление установкой в ОС Windows

Для управления установкой Kaspersky CyberTrace можно использовать исполняемый файл установщика.

Параметры исполняемого файла установщика

Исполняемый файл установщика обеспечивает следующие возможности:

- Установка Kaspersky CyberTrace

  Чтобы установить Kaspersky CyberTrace, запустите исполняемый файл установщика и следуйте инструкциям мастера установки Kaspersky CyberTrace.

- Удаление Kaspersky CyberTrace

  Если ПО Kaspersky CyberTrace уже установлено, при запуске исполняемого файла установщика становится доступной кнопка **Remove** в мастере установки Kaspersky CyberTrace. При нажатии на эту кнопку Kaspersky CyberTrace удаляется с сервера.

  При удалении установленного ПО также удаляются все подкаталоги и файлы в каталоге установки.

- Изменение конфигурации Kaspersky CyberTrace

  Если ПО Kaspersky CyberTrace уже установлено, при запуске исполняемого файла установщика становится доступной кнопка **Change** в мастере установки Kaspersky CyberTrace. Нажатие на эту кнопку позволяет изменить конфигурацию установленного ПО Kaspersky CyberTrace. Эта возможность позволяет изменить настройки установки или принять необходимые меры в случае, если список доступных потоков данных об угрозах изменился.

  Чтобы получить возможность перенастроить установку Kaspersky CyberTrace, запустите исполняемый файл установщика с правами Администратора.

Действия в случае ошибки при установке

Во время установки после остановки Kaspersky CyberTrace Service конфигурационные файлы и некоторые другие файлы перемещаются во временный каталог $TEMP\cybertrace_old. Если во время установки возникают ошибки, перемещенные файлы остаются в этом временном каталоге.

Для определения местоположения каталога `$TEMP` исполняемый файл установщика Kaspersky CyberTrace использует первую существующую переменную из следующего списка: %TMP%, %TEMP%, %USERPROFILE%, %WINDIR%. Исполняемый файл установщика пытается выполнить запись в этот каталог. Если попытка записи не удалась, исполняемый файл установщика осуществляет запись в каталог `%WINDIR%\Temp`.

Файл журнала обновления расположен во временном каталоге пользователя, запустившего установщик, или в каталоге, указанном в переменной среды `$TEMP` (см. выше).

Если в ходе автоматического обновления возникла ошибка, обратитесь по адресу intelligence@kaspersky.com для получения дополнительной информации о способах решения проблемы.

Обновление предыдущей версии Kaspersky CyberTrace

В этом разделе описывается порядок обновления Kaspersky CyberTrace до версии 5.4.

Обновить Kaspersky CyberTrace до версии 5.4 можно только с версии 5.3.

О процессе обновления

Описываемый в этом разделе порядок обновления относится к Kaspersky CyberTrace версии 3.1.0 и выше. Консультацию по обновлению более старой версии Kaspersky CyberTrace или Kaspersky Threat Feed Service можно получить у менеджера по работе с клиентами.

Обновление Kaspersky CyberTrace осуществляется в два этапа:

- Обновление бинарных и иных файлов.
- Обновление интеграции Kaspersky CyberTrace с SIEM-системой.

  Этот шаг не актуален для Log Scanner.

Как узнать версию Kaspersky CyberTrace

Версию Kaspersky CyberTrace можно узнать следующим образом:

- В Windows обратите внимание на свойство версии исполняемого файла kl_feed_service.exe.
- В Linux выполните следующую команду:

  ```
  %service_dir%/bin/kl_feed_service -v
  ```

Автоматическое обновление в ОС Linux

В этом разделе описывается порядок обновления Kaspersky CyberTrace в ОС Linux.

Приведенная ниже инструкция относится к установке пакетов RPM/DEB.

Автоматическое обновление доступно только в том случае, если для обновляемого установленного ПО принято лицензионное соглашение.

Чтобы автоматически обновить Kaspersky CyberTrace до более новой версии, выполните следующие действия:

1. Выполните следующую команду с правами root:

   ```
   run.sh upgrade
   ```

2. В начале процесса обновления ответьте утвердительно на запрос на остановку Kaspersky CyberTrace Service. Если отказаться от остановки, продолжить обновление невозможно.

   В конце процедуры обновления все параметры, данные учетных записей пользователей, доступные потоки данных об угрозах и сертификаты автоматически переносятся в новую версию.

   > После завершения процесса обновления для новых потоков данных об угрозах, которые не поддерживались в предыдущей версии, поля контекста не будут заданы. При необходимости задайте эти поля вручную на странице **Параметры → Потоки данных**.

   После завершения процесса обновления автоматически запускается Kaspersky CyberTrace Service.

> Если не удается обновить приложение до более новой версии, Kaspersky CyberTrace выполнит откат к версии, которая была работоспособна на момент начала обновления.

Действия в случае ошибки при обновлении

Во время обновления после остановки Kaspersky CyberTrace Service конфигурационные файлы и некоторые другие файлы перемещаются во временный каталог `/opt/kaspersky_cybertrace_tmp`. Если во время обновления возникают ошибки, перемещенные файлы остаются в этом временном каталоге.

Файл журнала обновления находится в каталоге `/temp` или в каталоге, указанном в переменной среды `$TEMP`, если переменная `$TEMP` определена.

Если в ходе автоматического обновления возникла ошибка, обратитесь по адресу intelligence@kaspersky.com для получения дополнительной информации о способах решения проблемы.

Автоматическое обновление в ОС Windows

В этом разделе описывается порядок обновления Kaspersky CyberTrace в ОС Windows.

Приведенная ниже инструкция применима к установке, выполняемой с помощью исполняемого файла установщика.

> Автоматическое обновление с помощью исполняемого файла установщика доступно только в том случае, если для обновляемого установленного ПО принято лицензионное соглашение.

Чтобы автоматически обновить Kaspersky CyberTrace до более новой версии, выполните следующие действия:

1. Запустите исполняемый файл установщика, который автоматически запустит процесс обновления.
2. В начале процесса обновления ответьте утвердительно на запрос на остановку Kaspersky CyberTrace Service. Если отказаться от остановки, продолжить обновление невозможно.

   Если Kaspersky CyberTrace Service остановлен и обновление продолжается, все параметры, данные учетных записей пользователей, доступные потоки данных об угрозах и сертификаты автоматически переносятся в новую версию.

   > После завершения процесса обновления для новых потоков данных об угрозах, которые не поддерживались в предыдущей версии, поля контекста не будут заданы. При необходимости задайте эти поля вручную на странице **Параметры → Потоки данных**.

3. При необходимости измените настройки в процессе обновления.

После завершения процесса обновления автоматически запускается Kaspersky CyberTrace Service.

> Если не удается обновить приложение до более новой версии, Kaspersky CyberTrace выполнит откат к версии, которая была работоспособна на момент начала обновления.

Действия в случае ошибки при обновлении

Во время обновления после остановки Kaspersky CyberTrace Service конфигурационные файлы и некоторые другие файлы перемещаются во временный каталог `$TEMP\cybertrace_old`. Если во время обновления возникают ошибки, перемещенные файлы остаются в этом временном каталоге.

Для определения местоположения каталога `$TEMP` исполняемый файл установщика Kaspersky CyberTrace использует первую существующую переменную из следующего списка: `%TMP%`, `%TEMP%`, `%USERPROFILE%`, `%WINDIR%`. Исполняемый файл установщика пытается выполнить запись в этот каталог. Если попытка записи не удалась, исполняемый файл установщика осуществляет запись в каталог `%WINDIR%\Temp`.

Файл журнала обновления расположен во временном каталоге пользователя, запустившего установщик, или в каталоге, указанном в переменной среды `$TEMP` (см. выше).

Если в ходе автоматического обновления возникла ошибка, обратитесь по адресу intelligence@kaspersky.com для получения дополнительной информации о способах решения проблемы.

Изменения после обновления

После обновления при первом входе в веб-интерфейс Kaspersky CyberTrace открывается окно Положение о KSN. Чтобы продолжить использование Kaspersky CyberTrace, примите или отклоните Положение о KSN в актуальной редакции. В дальнейшем вы сможете изменить соответствующий статус на странице **Параметры** → **Служба** в режиме **Управление системой**.

После обновления Kaspersky CyberTrace выполняются следующие изменения:

- Страница **Поиск** в веб-интерфейсе Kaspersky CyberTrace и многопользовательский режим становятся доступны на уровне лицензирования Matching Engine.
- В режиме **Управление системой** в раздел **Безопасность** добавлена страница **Параметры**. На этой странице можно настроить аудит действий пользователей.
- В режиме **Управление системой** количество потоков исполнения для анализа отображается на странице **Параметры** → **Ретроскан**.

Обновление интеграции Kaspersky CyberTrace (QRadar)

В этом разделе описывается порядок завершения интеграции Kaspersky CyberTrace с QRadar после обновления файлов Kaspersky CyberTrace.

Обновление интеграции Kaspersky CyberTrace с QRadar вручную

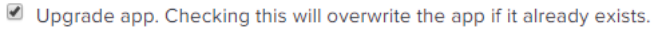
Чтобы обновить интеграцию Kaspersky CyberTrace с QRadar вручную, выполните следующие действия:

Выполните действия, описанные в разделах Импорт QID в QRadar, Отправка набора событий в QRadar и Сопоставление событий с QID для категорий и событий, перечисленных выше. Можно использовать файлы `sample_initiallog.txt` и `sample_qid.txt`, входящие в комплект поставки Kaspersky CyberTrace.

Обновление интеграции Kaspersky CyberTrace (Splunk)

В этом разделе описывается порядок завершения интеграции Kaspersky CyberTrace со Splunk после обновления Kaspersky CyberTrace.

При обновлении интеграции Kaspersky CyberTrace со Splunk до последней версии необходимо импортировать в Splunk новую версию приложения Kaspersky CyberTrace App for Splunk. Во время импорта выберите вариант, показанный на рисунке ниже.



Обновление интеграции со Splunk

Настройки приложения сбрасываются. Старые настройки будут сохранены в каталоге `%SPLUNK_DIRECTORY%/etc/apps/Kaspersky-CyberTrace-App-for-Splunk/default.old.%CURRENT_DATE%`, где `%CURRENT_DATE%` может задаваться в формате `ггггммдд-ччммсс` (например, `20190725-161423`). Приложение Kaspersky CyberTrace App for Splunk должно быть настроено полностью в соответствии с конфигурацией старой версии.

Обновление интеграции Kaspersky CyberTrace (ArcSight)

В этом разделе описывается порядок завершения интеграции Kaspersky CyberTrace с ArcSight после обновления файлов Kaspersky CyberTrace.

При обновлении интеграции Kaspersky CyberTrace с ArcSight до последней версии необходимо импортировать новую версию пакета ARB. Во время импорта необходимо принять обновление текущего пакета ARB.

Обновление интеграции Kaspersky CyberTrace (RSA)

В этом разделе описывается порядок завершения интеграции Kaspersky CyberTrace с RSA NetWitness после обновления файлов Kaspersky CyberTrace.

При обновлении интеграции Kaspersky CyberTrace с RSA NetWitness до последней версии необходимо импортировать файлы `cybertrace.ini` и `v20_cybertracemsg.xml` из каталога `%service_dir%/integration/rsa/cybertrace` в Log Decoder. После импорта перезапустите Log Decoder.

> Если обновляется файл `v20_cybertracemsg.xml`, убедитесь, что поля контекста указаны для всех используемых потоков данных об угрозах.

Обновление интеграции Kaspersky CyberTrace (LogRhythm)

В этом разделе описывается порядок завершения интеграции Kaspersky CyberTrace с LogRhythm после обновления Kaspersky CyberTrace.

Завершение интеграции Kaspersky CyberTrace с LogRhythm состоит из следующих шагов:

- Добавление новых событий в LogRhythm
- Удаление устаревших событий из LogRhythm

Добавление новых событий

Чтобы добавить новые события в LogRhythm, выполните следующие действия:

Добавьте требуемые категории и оповещения о событиях автоматически или вручную (как описано в разделах Шаг 3 (необязательный). Добавление событий Kaspersky CyberTrace и Шаг 4 (необязательный). Добавление правил Kaspersky CyberTrace).

Удаление устаревших событий

Чтобы удалить устаревшие события из LogRhythm, выполните следующие действия:

1. Запустите LogRhythm Console.
2. Выберите **Deployment Manager** → **Tools** → **Knowledge** → **MPE Rule Builder**.

   Откроется форма **Rule Builder**.

3. Нажмите на кнопку **Open rule library** ( ).

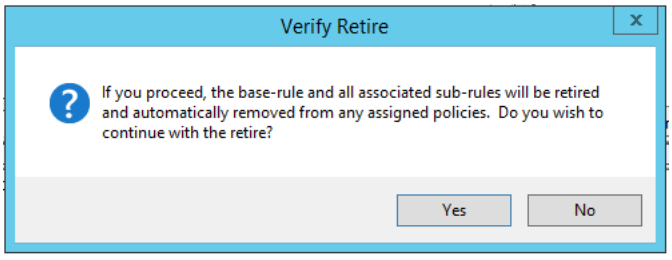
4. Для каждого устаревшего события выполните следующие действия:

   a. Дважды нажмите на правило, которое требуется удалить.

      Откроется окно предварительного просмотра правила.

   b. Нажмите на кнопку **Retire rule** ( ).

   c. В окне **Verify Retire** нажмите на кнопку **Yes**.



Окно «Verify Retire»

Удаление Kaspersky CyberTrace

В этом разделе описывается порядок удаления Kaspersky CyberTrace.

Удаление Kaspersky CyberTrace (Windows)

В этом разделе описывается порядок удаления Kaspersky CyberTrace в Windows. После удаления Kaspersky CyberTrace необходимо удалить связанные с ним объекты из используемой SIEM-системы.

Удаление Kaspersky CyberTrace (исполняемый файл установщика)

Ниже приведена процедура удаления экземпляра Kaspersky CyberTrace, установленного с помощью исполняемого файла установщика.

Чтобы удалить Kaspersky CyberTrace, выполните следующие действия:

1. Запустите исполняемый файл установщика Kaspersky CyberTrace.

   Запустится мастер установки Kaspersky CyberTrace.

2. Нажмите на кнопку **Remove**.

3. Следуйте инструкциям мастера.

Действия в случае ошибки при удалении

Если в ходе удаления возникла ошибка, обратитесь по адресу intelligence@kaspersky.com для получения дополнительной информации о способах решения проблемы.

Удаление Kaspersky CyberTrace (Linux)

В этом разделе описывается порядок удаления Kaspersky CyberTrace в Linux. После успешного удаления следует также удалить объекты, связанные с Kaspersky CyberTrace, из используемой SIEM-системы.

Удаление (RPM и DEB)

Ниже описан порядок удаления Kaspersky CyberTrace, установленного с помощью пакета DEB или RPM.

Чтобы удалить Kaspersky CyberTrace, выполните следующие действия:

1. Выполните следующую команду:

   ```
   %service_dir%/run.sh remove
   ```

2. Следуйте инструкциям мастера.

Действия в случае ошибки при удалении

Если в ходе удаления возникла ошибка, обратитесь по адресу intelligence@kaspersky.com для получения дополнительной информации о способах решения проблемы.

Удаление объектов Kaspersky CyberTrace (QRadar)

В этом разделе описывается порядок удаления объектов, связанных с Kaspersky CyberTrace, из QRadar после удаления Kaspersky CyberTrace. Обратите внимание, что после удаления этих объектов события из Kaspersky CyberTrace останутся в QRadar.

После удаления Kaspersky CyberTrace удалите приложение Kaspersky CyberTrace App for QRadar (если оно установлено). Если не планируется устанавливать Kaspersky CyberTrace в будущем, также можно удалить источники журналов, относящиеся к Kaspersky CyberTrace (это могут быть источники журналов `KL_Threat_Feed_Service_v2` и `KL_Verification_Tool`).

Чтобы удалить источник журналов из QRadar, выполните следующие действия:

1. В QRadar выберите **Admin**, а в разделе **Data Sources** выберите **Log Sources**.

   Откроется окно **Log Sources**.

2. Выберите источник журналов, который требуется удалить, и нажмите на кнопку **Delete**.

Удаление объектов Kaspersky CyberTrace (Splunk)

В этом разделе описывается порядок удаления объектов, связанных с Kaspersky CyberTrace, из Splunk после удаления Kaspersky CyberTrace. Обратите внимание, что после удаления этих объектов события из Kaspersky CyberTrace останутся в Splunk.

Чтобы удалить объекты, связанные с Kaspersky CyberTrace, после удаления Kaspersky CyberTrace, выполните следующие действия:

1. Удалите следующие каталоги:

   a. Для схемы интеграции с одним экземпляром: `%SPLUNK_HOME%/etc/apps/Kaspersky-CyberTrace-App-for-Splunk`.

   b. Для Search Head и Heavy Forwarder (распределенная схема интеграции): `%SPLUNK_HOME%/etc/apps/Kaspersky-CyberTrace-App-for-Splunk`.

   c. Для Universal Forwarder (распределенная схема интеграции): `%SPLUNK_HOME%/etc/apps/Splunk_TA_Kaspersky-CyberTrace-App-for-Splunk-Universal-Forwarder`, в котором расположено приложение Kaspersky CyberTrace App for Splunk.

   Здесь `%SPLUNK_HOME%` — это каталог, в который установлен Splunk.

2. Перезапустите Splunk. Перезапустить Splunk можно либо с помощью веб-интерфейса Splunk, либо следующей командой:

   ```
   %SPLUNK_HOME%/bin/splunk restart
   ```

После этого можно очистить Splunk от событий, полученных от Kaspersky CyberTrace.

Чтобы очистить Splunk от событий, полученных от Kaspersky CyberTrace, выполните следующие действия:

1. Запустите приложение **Search & Reporting**, для этого нажмите его кнопку веб-интерфейсе Splunk.

2. Удалите события из Kaspersky CyberTrace:

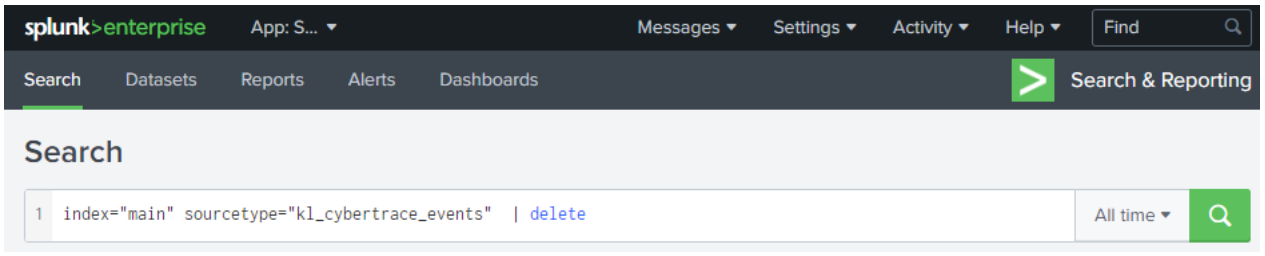
   a. В поле **Search** введите следующую команду:

   ```
   index="main" sourcetype="kl_cybertrace_events" | delete
   ```

   > Удаление событий из индекса `main` возможно только под учетной записью пользователя с ролью `can_delete`. Чтобы добавить эту роль в учетную запись пользователя, необходимо выбрать **Settings** → **Roles** в главном меню Splunk.

b. Рядом с полем **Search** в раскрывающемся списке выбора временного интервала событий для поиска выберите **All time**.

c. Нажмите на кнопку **Search**.



Приложение «Search & Reporting»

Удаление объектов Kaspersky CyberTrace (ArcSight)

В этом разделе описывается порядок удаления объектов, связанных с Kaspersky CyberTrace, из ArcSight после удаления Kaspersky CyberTrace. Обратите внимание, что после удаления этих объектов события из Kaspersky CyberTrace останутся в Splunk.

Чтобы удалить из ArcSight объекты, связанные с Kaspersky CyberTrace, выполните следующие действия:

1. Удалите пакет ARB из ArcSight.

   Для этого в ArcSight Console удалите пакет `/All Packages/Public/Kaspersky CyberTrace Connector`.

2. Удалите службу ArcSight SmartConnector, который использовался для получения событий от Kaspersky CyberTrace Service.

   В Linux это делается следующим образом:

   a. Остановите службу ArcSight SmartConnector следующей командой:

      `/etc/init.d/arc_%service_name% stop`

      Здесь `%service_name%` – это имя службы ArcSight SmartConnector, указанное при его установке.

   b. Выполните следующую команду, чтобы удалить ArcSight SmartConnector:

      `%ConnectorInstallDir%/UninstallerData/Uninstall_ArcSightAgents`

      Здесь `%ConnectorInstallDir%` – это каталог, в который был установлен ArcSight SmartConnector.

   c. Удалите каталог `%ConnectorInstallDir%`.

   В Windows служба ArcSight SmartConnector удаляется путем запуска приложения удаления ArcSight SmartConnector.

3. Удалите ArcSight Forwarding Connector, который использовался для отправки событий в Kaspersky CyberTrace Service.

   Это делается следующим образом:

   a. Остановите службу ArcSight Forwarding Connector следующей командой:

      `/etc/init.d/arc_%FORWARDING% stop`

      Здесь `%FORWARDING%` – это имя службы ArcSight Forwarding Connector, указанное при его установке.

b. Выполните следующую команду, чтобы удалить ArcSight Forwarding Connector:

`%ConnectorInstallDir%/UninstallerData/Uninstall_ArcSightAgents`

Здесь `%ConnectorInstallDir%` – это каталог, в который был установлен ArcSight Forwarding Connector.

c. Удалите каталог `%ConnectorInstallDir%`.

Удаление объектов Kaspersky CyberTrace (RSA NetWitness)

В этом разделе описывается порядок удаления объектов, связанных с Kaspersky CyberTrace, из RSA NetWitness после удаления Kaspersky CyberTrace. Обратите внимание, что после удаления этих объектов события из Kaspersky CyberTrace останутся в RSA NetWitness.

Чтобы удалить из RSA Net Witness объекты, связанные с Kaspersky CyberTrace, выполните следующие действия:

1. Удалите каталог `/etc/netwitness/ng/envision/etc/devices/cybertrace` на сервере, где работает Log Decoder.
2. В настройках Log Decoder удалите правило пересылки `cybertrace` аналогично тому, как оно было добавлено.
3. Если пересылка событий в будущем не планируется, отключите пересылку событий, для этого установите для параметра `/decoder/config/logs.forwarding.enabled` значение `false`.
4. Удалите информационную панель `Kaspersky_CyberTrace` аналогично тому, как информационная панель была создана.
5. Удалите диаграммы Kaspersky CyberTrace так же, как они были включены.
6. Удалите отчет `CyberTrace Report` аналогично тому, как он создается.
7. Удалите правила Kaspersky CyberTrace Service так же, как они были импортированы.
8. Если в файлы index-concentrator-custom.xml или table-map-custom.xml добавлялись поля, удалите их из этих файлов.
9. Перезапустите Concentrator, если в файл index-concentrator-custom.xml внесены изменения.
10. Перезапустите Log Decoder.

Добавление самоподписанных SSL-сертификатов для веб-интерфейса Kaspersky CyberTrace

Сертификат SSL и закрытый ключ, сгенерированные во время установки Kaspersky CyberTrace, позволяют использовать веб-интерфейс Kaspersky CyberTrace по HTTPS. Сертификат является самоподписанным, поэтому используемый браузер предупреждает о небезопасном соединении. Рекомендуется использовать сертификат, который является доверенным в вашей инфраструктуре. Однако, если использование доверенного сертификата невозможно, можно добавить самоподписанный сертификат в качестве доверенного для браузера или операционной системы.

Повторное создание SSL-сертификатов и добавление доверенных сертификатов для веб-интерфейса Kaspersky CyberTrace

Веб-интерфейс Kaspersky CyberTrace использует SSL-сертификат для HTTPS-соединений. По умолчанию веб-интерфейс Kaspersky CyberTrace использует самоподписанный сертификат и закрытый ключ, которые генерируются во время установки Kaspersky CyberTrace.

Сгенерированный сертификат действителен в течение двух лет. Если срок его действия истечет, можно повторно создать новый сертификат SSL с помощью конфигуратора (в Linux) или исполняемого файла установщика (в Windows).

Рекомендуется использовать сертификат, который будет доверенным в вашей инфраструктуре, а затем настроить в Kaspersky CyberTrace использование этого сертификата вместо самоподписанного сертификата.

> Перед внесением изменений создайте резервную копию существующего закрытого ключа, сертификата и конфигурационного файла Kaspersky CyberTrace Service.

Чтобы повторно создать самоподписанный SSL-сертификат для веб-интерфейса Kaspersky CyberTrace:

- В ОС Linux:

  a. Выполните в консоли следующую команду:

  ```
  %service_dir%/bin/configure --change
  ```

  b. Перезапустите Kaspersky CyberTrace Service:

  ```
  systemctl restart cybertrace
  ```

- В ОС Windows:

  a. Запустите исполняемый файл установщика Kaspersky CyberTrace.

  b. Нажмите на кнопку **Change**.

  c. Перезапустите Kaspersky CyberTrace с помощью Диспетчера управления службами (SCM):

```
sc stop cybertrace
sc start cybertrace
```

Чтобы добавить доверенный сертификат для веб-интерфейс Kaspersky CyberTrace:

1. Убедитесь, что сертификат соответствует необходимым требованиям безопасности.

   Для установления TLS-соединения могут применяться следующие наборы шифров:

   ECDHE-RSA-AES256-GCM-SHA384

   ECDHE-RSA-AES128-GCM-SHA256

   ECDHE-ECDSA-AES128-GCM-SHA256

   ECDHE-ECDSA-AES256-GCM-SHA384

   ECDHE-RSA-CHACHA20-POLY1305

   Допускается применение TLS 1.2 и 1.3.

2. Преобразуйте закрытый ключ и доверенный сертификат в формат PEM.

3. При необходимости отредактируйте элементы `ServiceSettings` > `Security` > `TLS` > `SSLCertificatePath` и `ServiceSettings` > `Security` > `TLS` > `SSLPrivateKeyPath` конфигурационного файла Kaspersky CyberTrace Service, чтобы они содержали пути к сертификату и закрытому ключу, соответственно.

   Сохраните конфигурационный файл Kaspersky CyberTrace Service.

4. Перезапустите Kaspersky CyberTrace Service.

Сертификаты также используются для установления TLS-соединения с SIEM, поэтому их изменение может повлиять на взаимодействие Kaspersky CyberTrace с SIEM (при настройке для работы через TLS), а не только на доступ к веб-интерфейсу.

Добавление самоподписанного сертификата в браузер как доверенного

В этом разделе описывается порядок добавления самоподписанных сертификатов, созданных при установке Kaspersky CyberTrace, в доверенное хранилище. Таким образом устраняются предупреждения о безопасности, выдаваемые браузерами.

Информация в этом разделе применима к ситуации, когда пользователь работает с веб-интерфейсом Kaspersky CyberTrace с того же сервера, на котором запущен веб-интерфейс Kaspersky CyberTrace. Если элемент `ServiceSettings → HTTPServer → ConnectionString` в конфигурационном файле Kaspersky CyberTrace Service ссылается на внешний интерфейс, веб-интерфейс Kaspersky CyberTrace не будет считаться доверенным, поскольку самоподписанный сертификат может использоваться только с адресами `https://127.0.0.1` и `https://localhost`.

Чтобы избежать потенциальных угроз безопасности, рекомендуется использовать доверенный сертификат, подписанный центром сертификации (ЦС).

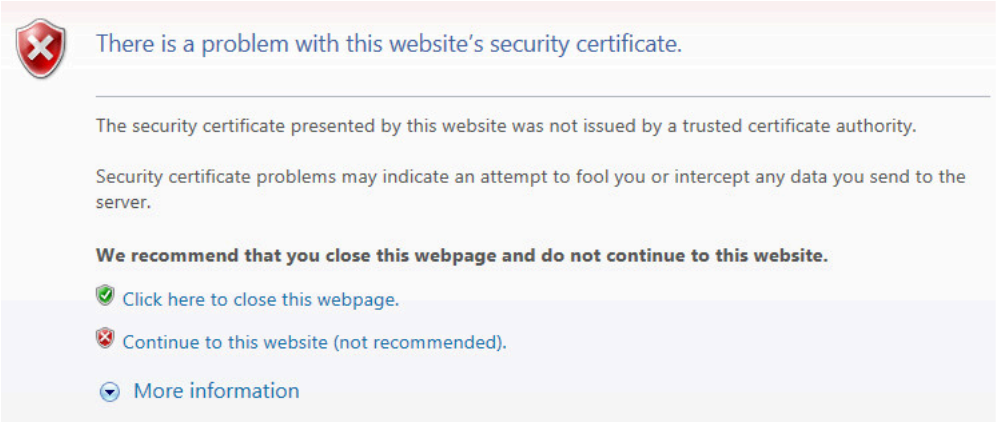
Придание самоподписанному сертификату доверенного статуса в браузере (веб-интерфейс Kaspersky CyberTrace открывается в Internet Explorer, установленном в системе Windows)

Придание сертификату доверенного статуса в браузере требует последовательного выполнения следующих трех процедуры:

Чтобы сохранить сертификат в локальный файл, выполните следующие действия:

1. Откройте адрес `https://127.0.0.1` или `https://localhost` в Internet Explorer®.

   Браузер сообщает о проблеме с сертификатом безопасности веб-сайта.



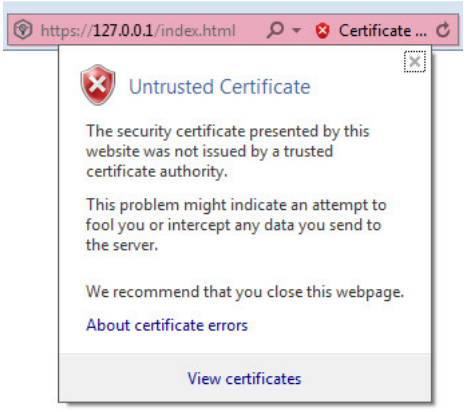
Сообщение об ошибке сертификата

2. Выберите ссылку **Continue to this website (not recommended)**.

   В адресной строке появляется сообщение **Ошибка сертификата**.

3. Нажмите на сообщение **Certificate Error**.

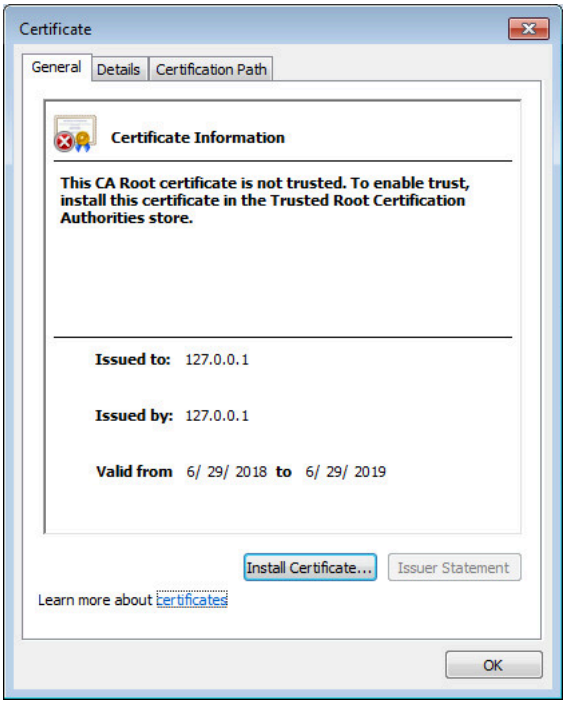
   Откроется окно **Untrusted Certificate**.



Окно **Untrusted Certificate**

4. Выберите ссылку **View certificates**.

Откроется окно **Certificate** с информацией о сертификате Kaspersky CyberTrace.



Окно **Certificate**

5. Выберите вкладку **Details** и нажмите **Copy to File**, чтобы создать локальную копию сертификата.

   Запустится мастер экспорта сертификата.



Мастер экспорта сертификатов

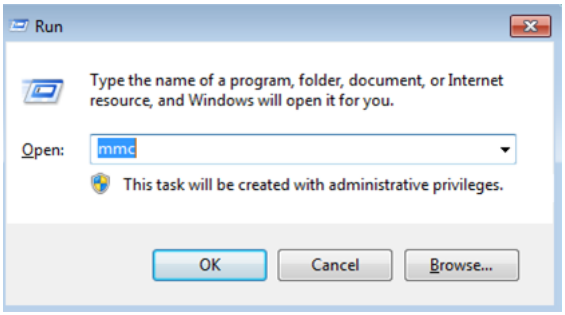
6. Следуйте инструкциям мастера.

   При экспорте сертификата используйте настройки мастера по умолчанию.

Чтобы запустить процесс импорта сертификата через Microsoft Management Console (MMC), выполните следующие действия:

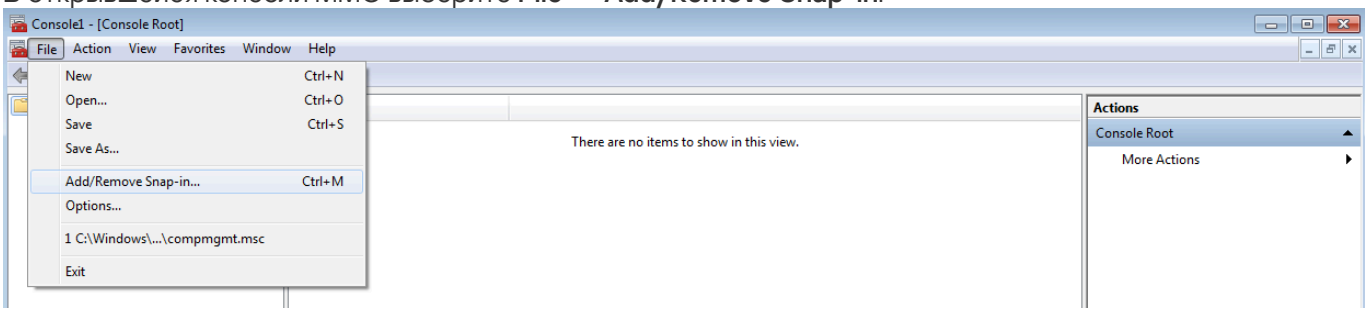
1. Из поля **Search** перейдите в поле **Run** и введите `mmc`.

Теперь можно запустить MMC от имени администратора.



Запуск MMC

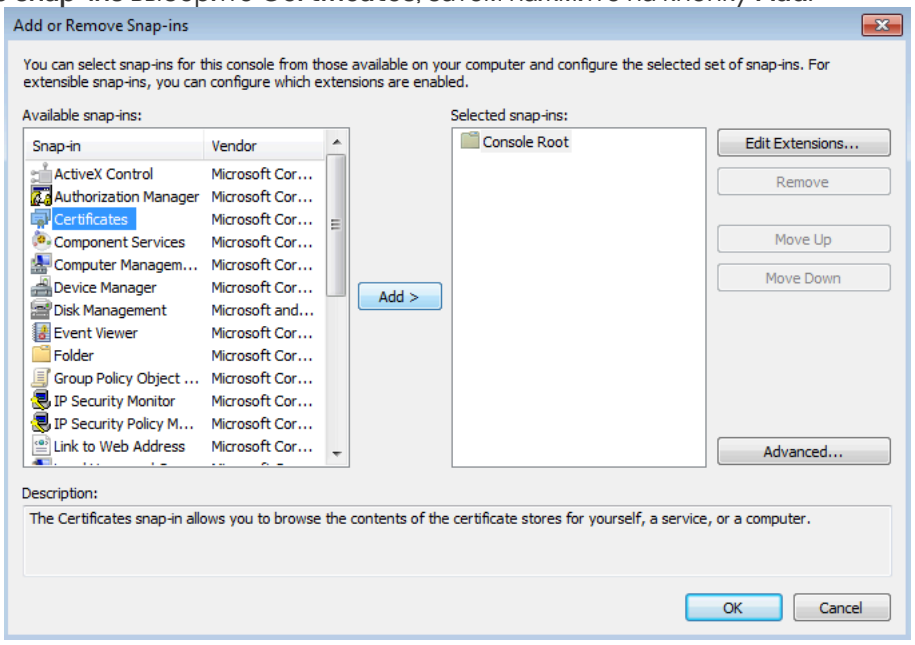
2. В открывшейся консоли MMC выберите **File → Add/Remove Snap-in**.



Выбор **Add/Remove Snap-in**

Откроется окно **Add or Remove Snap-ins**.

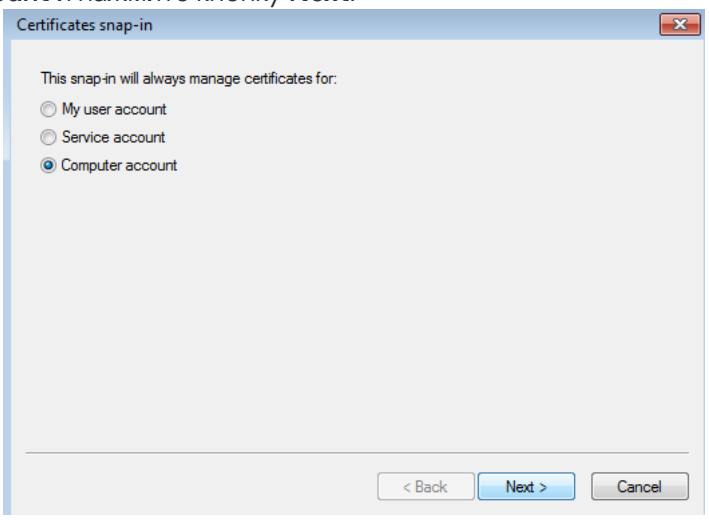
3. В списке **Available snap-ins** выберите **Certificates**, затем нажмите на кнопку **Add**.



Добавление оснастки сертификатов

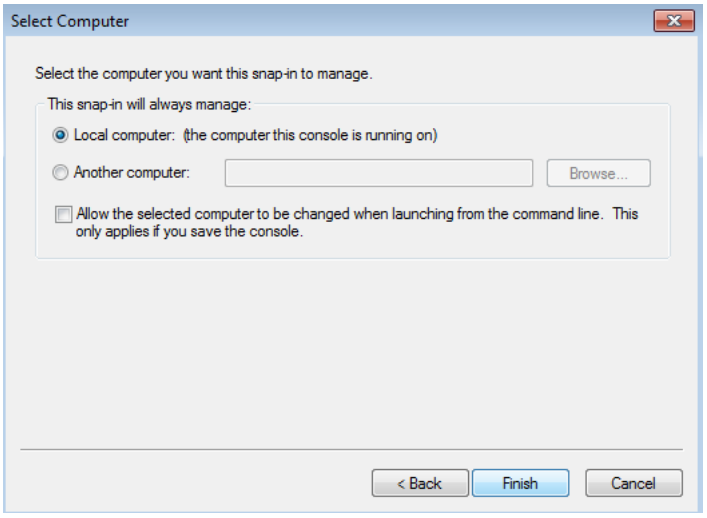
Откроется окно **Certificates snap-in**.

4. Выберите **Computer account** и нажмите кнопку **Next**.



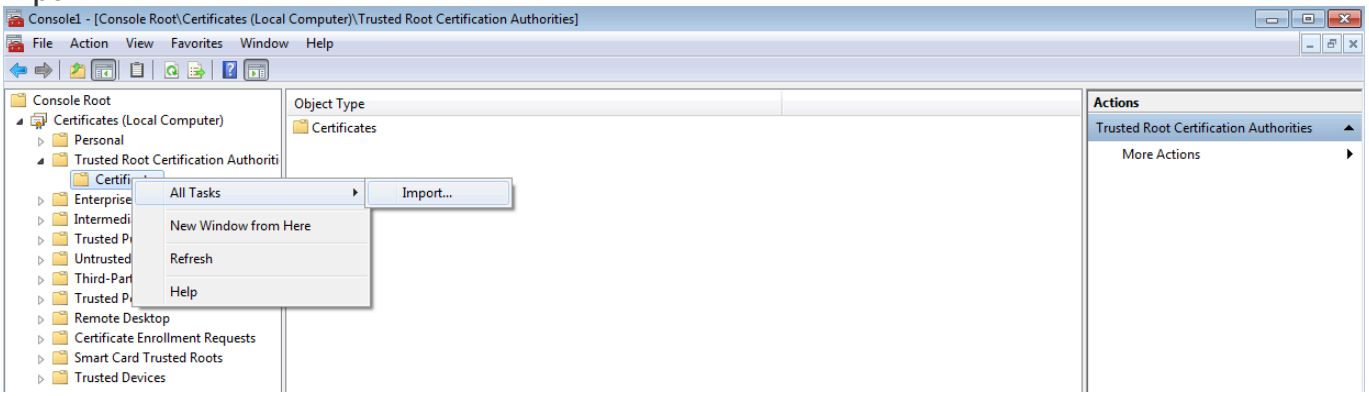
Выберите **Computer account**

В открывшемся окне **Select Computer** нажмите на кнопку **Finish**.



Выбор **Local computer**

5. В дереве выберите **Certificates (Local Computer)** → **Trusted Root Certification Authorities**, нажмите правой кнопкой мыши на элемент **Certificates**, затем выберите пункт контекстного меню **All Tasks** → **Import**.



Выбор **Import**

Запустится мастер импорта сертификата.

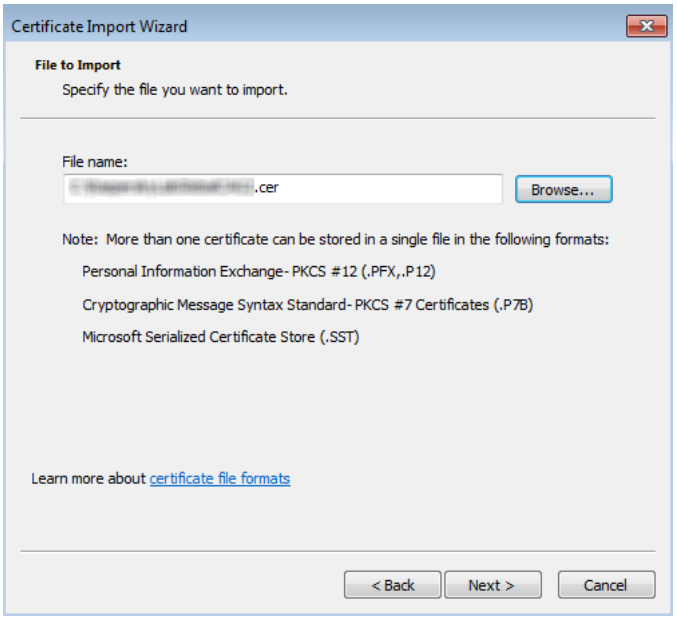
Чтобы добавить сохраненный сертификат в хранилище доверенных корневых центров сертификации, выполните следующие действия:

1. На странице приветствия мастера нажмите на кнопку **Next**.



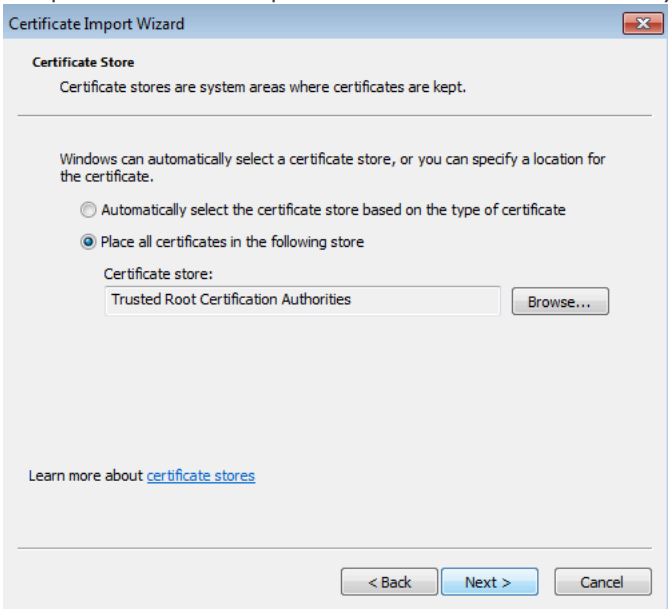
Мастер импорта сертификатов

2. Нажмите кнопку **Browse** и выберите сертификат, который был сохранен в описанной выше процедуре «Чтобы сделать самоподписанный сертификат для веб-интерфейса Kaspersky CyberTrace доверенным при использовании Google Chrome».



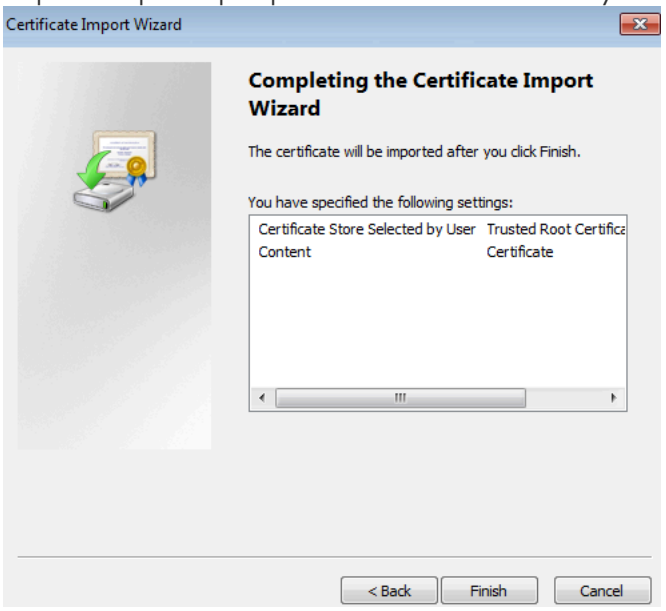
Импорт ранее сохраненного сертификата

3. На следующей странице мастера «Certificate Import Wizard» нажмите на кнопку **Next**.



Выбор хранилища сертификатов

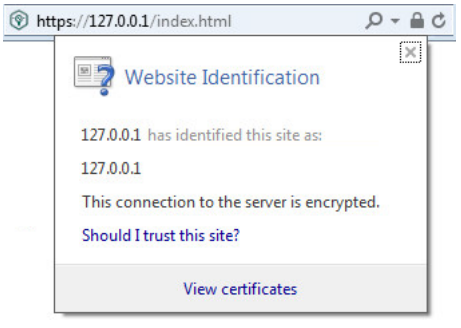
4. На последней странице мастера импорта сертификатов нажмите на кнопку **Finish**.



Завершение импорта сертификата

5. Закройте консоль на основе MMC и перезапустите браузер.

   Проблема безопасности (недоверенный сертификат) устранена, как показано на рисунке ниже.



Website identification

Придание самоподписанному сертификату доверенного статуса в браузере (веб-интерфейс Kaspersky CyberTrace открывается в Google Chrome, установленном в системе Windows)

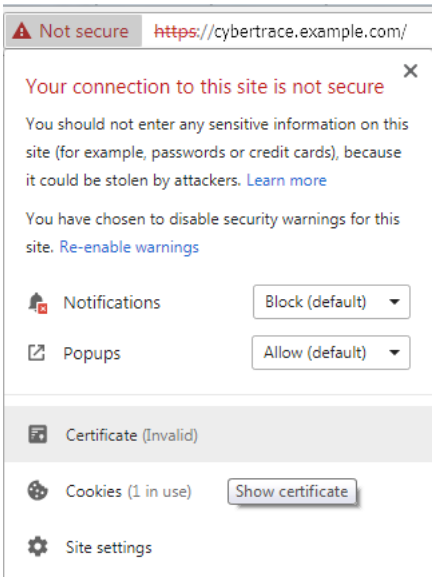
Чтобы сделать самоподписанный сертификат для веб-интерфейса Kaspersky CyberTrace доверенным при использовании Google Chrome:

1. Откройте адрес `https://127.0.0.1` или `https://localhost` в Google Chrome.

   В адресной строке отображается предупреждение о том, что соединение с сайтом небезопасно.

2. Нажмите на сообщение **Not secure**.

   Откроется окно со сведениями о безопасности веб-сайта.



Сведения о безопасности

3. Нажмите **Certificate**, чтобы просмотреть информацию о сертификате. (При наведении указателя мыши на **Certificate** отображается всплывающая подсказка **Show certificate**).

4. В открывшемся окне **Certificate** выберите вкладку **Details** и нажмите **Copy to File**, чтобы создать локальную копию сертификата.

Запустится мастер экспорта сертификата.



Мастер экспорта сертификатов

5. Следуйте инструкциям мастера.

   При экспорте сертификата используйте настройки мастера по умолчанию.

6. После сохранения сертификата на локальном диске откройте его и добавьте в хранилище доверенных корневых центров сертификации, как описано в процедуре для Internet Explorer.

7. Перезагрузите браузер.

Придание самоподписанному сертификату доверенного статуса в браузере (веб-интерфейс Kaspersky CyberTrace открывается в Mozilla Firefox)

Добавление веб-интерфейса Kaspersky CyberTrace в список доверенных веб-адресов Mozilla Firefox выполняется, чтобы в браузере не отображались предупреждения о сертификате.

Придание самоподписанному сертификату доверенного статуса в браузере (веб-интерфейс Kaspersky CyberTrace открывается в браузере для Linux)

Процедуры импорта сертификата как доверенного с помощью браузера (в системах Linux) различаются в зависимости от используемого браузера и дистрибутива Linux. Однако в этих процедурах есть общие шаги: открытие формы настроек браузера и использование этой формы для импорта сертификата в хранилище.

Чтобы вручную придать самоподписанному сертификату статус доверенного для браузера в системе Linux, выполните следующие действия:

1. Создайте каталог `/usr/local/share/ca-certificates/`, если он не существует на сервере:

   ```
   mkdir /usr/local/share/ca-certificates/
   ```

2. Скопируйте корневой сертификат (файл .crt) в созданный каталог:

   ```
   cp <полный путь к сертификату> /usr/local/share/ca-certificates/
   ```

3. Обновите сертификаты:

   ```
   sudo update-ca-certificates
   ```

> Если у пакет ca-certificates не установлен, установите его с помощью используемого в системе менеджера пакетов.

Удаление сертификата из списка доверенных

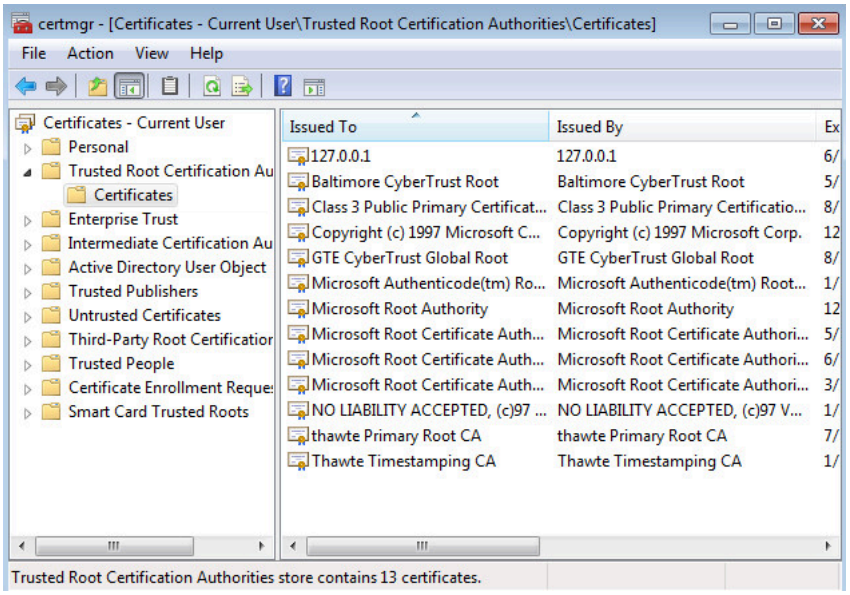
После перенастройки или удаления Kaspersky CyberTrace старые сертификаты больше не используются в Kaspersky CyberTrace. Их можно удалить из списка доверенных сертификатов.

Чтобы удалить сертификат из списка доверенных сертификатов (в Windows), выполните следующие действия:

1. Откройте консоль управления сертификатами и выполните следующую команду:

   ```
   certmgr.msc
   ```

2. В дереве выберите **Trusted Root Certification Authorities → Certificates**.



Консоль управления сертификатами

3. В области результатов щелкните добавленный сертификат правой кнопкой мыши и выберите команду **Delete**.

В системе Linux процедура удаления выполняется аналогично добавлению сертификата: откройте список доверенных сертификатов и удалите ненужные.

Токен доступа для Kaspersky Threat Intelligence Portal

Для выполнения некоторых трансформаций Kaspersky CyberTrace требуется токен доступа для подключения к Kaspersky Threat Intelligence Portal.

Получение токена доступа от Kaspersky Threat Intelligence Portal

Чтобы получить токен доступа от Kaspersky Threat Intelligence Portal, выполните следующие действия:

1. Купите коммерческую лицензию. Чтобы купить коммерческую лицензию, обратитесь в «Лабораторию Касперского» по адресу intelligence@kaspersky.com и следуйте указаниям менеджеров по работе с клиентами.
2. Примите Условия использования и Положение о предоставлении данных в вашем личном кабинете на портале Kaspersky Threat Intelligence Portal.
3. Получите токен доступа на странице настроек в вашем личном кабинете на портале Kaspersky Threat Intelligence Portal.

Добавление токена доступа в Kaspersky CyberTrace

Чтобы добавить токен доступа в Kaspersky CyberTrace, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите на страницу **Графы расследования**.
2. Нажмите на кнопку ⚙ (**Параметры**).

   Откроется окно **Параметры**.
3. В разделе **Kaspersky Threat Intelligence Portal API**, в поле **Токен доступа** введите токен доступа, используемый для подключения к API Kaspersky Threat Intelligence Portal.
4. Нажмите на кнопку **Сохранить**.

Kaspersky CyberTrace будет использовать указанный токен доступа для добавления в граф информации из Kaspersky Threat Intelligence Portal, когда пользователь запускает трансформацию этого рода.

Токен доступа для плагина VirusTotal

Для выполнения некоторых трансформаций Kaspersky CyberTrace требуется токен доступа для подключения к плагину VirusTotal.

Чтобы добавить токен доступа в Kaspersky CyberTrace, выполните следующие действия:

1. В веб-интерфейсе Kaspersky CyberTrace перейдите на страницу **Графы расследования**.
2. Нажмите на кнопку ⚙ (**Параметры**).

   Откроется окно **Параметры**.
3. В разделе **VirusTotal API**, в поле **Токен доступа** введите токен доступа, используемый для подключения к API VirusTotal.
4. Нажмите на кнопку **Сохранить**.

Kaspersky CyberTrace будет использовать указанный токен доступа для добавления в граф информации из плагина VirusTotal, когда пользователь запускает трансформации VirusTotal.

Проверка соединения с Kaspersky CyberTrace Service и наличия потоков данных об угрозах

В этом разделе описывается порядок проверки соединения с Kaspersky CyberTrace Service и способности Kaspersky CyberTrace Service сопоставлять события с определенными потоками данных об угрозах.

Перед проверкой соединения с Kaspersky CyberTrace Service необходимо убедиться, что в элементе `ServiceSettings > ScannersCount` конфигурационного файла есть хотя бы один неиспользуемый сканер.

Отправка ping-запроса

Для проверки соединения с Kaspersky CyberTrace Service можно отправить ping-запрос. Этот метод не требует, чтобы какие-либо потоки данных об угрозах были включены. Для использования этого метода не потребуется коммерческий сертификат для доступа к потокам данных об угрозах от «Лаборатории Касперского» Kaspersky Threat Data Feeds.

Чтобы проверить соединение с Kaspersky CyberTrace Service путем отправки ping-запроса, выполните следующие действия:

1. Установите TCP-соединение с использованием IP-адреса и порта, которые Kaspersky CyberTrace Service прослушивает для получения входящих событий.
2. Отправьте `X-KF-ReplyBackPING` в качестве первого сообщения.
3. Дождитесь ответа.

Если в ответ приходит `PONG`, это означает, что Kaspersky CyberTrace Service работает и прослушивает указанные IP-адрес и порт в ожидании входящих событий.

Отправка тестового события

Кроме реальных индикаторов компрометации, потоки данных об угрозах Kaspersky Threat Data Feeds также содержат записи, предназначенные только для тестирования, и не соответствующие реальным вредоносным объектам. С помощью данных записей можно убедиться в корректности функционирования Kaspersky CyberTrace Service в части сопоставления входящих событий с потоками данных об угрозах Kaspersky Threat Data Feeds. Эти записи всегда присутствуют в потоках данных об угрозах Kaspersky Threat Data Feeds и никогда не удаляются.

Чтобы проверить соединение с Kaspersky CyberTrace Service путем отправки тестового события, выполните следующие действия:

1. Установите TCP-соединение с использованием IP-адреса и порта, которые Kaspersky CyberTrace Service прослушивает для получения входящих событий.

2. Отправьте `X-KF-SendFinishedEventX-KF-ReplyBack` в качестве первого сообщения.

3. Отправьте тестовое событие, содержащее тестовую запись для конкретного потока данных об угрозах из таблиц, приведенных ниже.

   В следующей таблице приведены тестовые записи для коммерческих потоков данных об угрозах.

Тестовые записи (коммерческие потоки данных об угрозах)

Используемый поток данных об угрозах	Тестовые записи	Категория события
Malicious URL Data Feed	http://fakess123.nu	KL_Malicious_URL
Phishing URL Data Feed	http://fakess123ap.nu	KL_Phishing_URL
Botnet C&C URL Data Feed	http://fakess123bn.nu	KL_BotnetCnC_URL
IP Reputation Data Feed	192.0.2.1	KL_IP_Reputation
Malicious Hash Data Feed	FEAF2058298C1E174C2B79AFFC7CF4DF	KL_Malicious_Hash_MD5
Mobile Malicious Hash Data Feed	60300A92E1D0A55C7FDD360EE40A9DC1	KL_Mobile_Malicious_Hash_MD5
Mobile Botnet C&C URL Data Feed	http://sdfed7233dsfg93acvbhl.su/steallallsms.php	KL_Mobile_BotnetCnC_URL
Ransomware URL Data Feed	http://fa7830b4811fbef1b187913665e6733c.com	KL_Ransomware_URL
APT URL Data Feed	http://b046f5b25458638f6705d53539c79f62.com	KL_APT_URL
APT Hash Data Feed	7A2E65A0F70EE0615EC0CA34240CF082	KL_APT_Hash_MD5
APT IP Data Feed	192.0.2.4	KL_APT_IP
IoT URL Data Feed	http://e593461621ee0f9134c632d00bf108fd.com/.i	KL_IoT_URL
ICS Hash Data Feed	7A8F30B40C6564EFF95E678F7C43346C	KL_ICS_Hash_MD5

В следующей таблице приведены тестовые записи, которые можно использовать, когда включены только демонстрационные потоки данных об угрозах.

Тестовые записи (демонстрационные потоки данных об угрозах)

Используемый поток данных об угрозах	Тестовые записи	Категория события
DEMO Botnet_CnC_URL_Data_Feed	http://5a015004f9fc05290d87e86d69c4b237.com	KL_BotnetCnC_URL
DEMO IP_Reputation_Data_Feed	192.0.2.1	KL_IP_Reputation
DEMO Malicious_Hash_Data_Feed	776735A8CA96DB15B422879DA599F474	KL_Malicious_Hash_MD5

4. Дождитесь ответа.

- Если ответ представляет собой оповещение об обнаружении индикаторов компрометации, содержащее соответствующую категорию события из приведенных выше таблиц, это означает, что служба Kaspersky CyberTrace может получать события и сопоставлять их с конкретным потоком данных об угрозах.

- Если же приходит ответ `LookupFinished` без информации о событии, это означает, что Kaspersky CyberTrace Service может получать события и выполнять сопоставление, но конкретный поток данных об угрозах отключен.

Руководства для разработчиков

В этой главе представлена информация о разработке приложений, взаимодействующих с Kaspersky CyberTrace.

Учебное руководство по разработке приложения на Python: часть 1

В этом руководстве описывается реализация обмена данными с Kaspersky CyberTrace в приложении на Python.

В части 1 этого руководства описывается приложение, отправляющее данные в Kaspersky CyberTrace.

В части 2 этого руководства описывается приложение, ожидающее получения событий от Kaspersky CyberTrace.

Введение

Эта часть руководства посвящена реализации приложения Python, отправляющего данные в Kaspersky CyberTrace. Kaspersky CyberTrace анализирует полученные данные, сопоставляя их с индикаторами. Если сопоставление обнаруживает совпадающие индикаторы, Kaspersky CyberTrace отправляет в ответ свои собственные события.

Для приложения можно использовать любое имя. В примерах в этом руководстве для этого приложения используется имя файла `send_events_cybertrace.py`.

> Для реализации этого приложения рекомендуется использовать Python 3. В этом руководстве в примерах кода используется синтаксис Python 3.

О флаге X-KF-ReplyBack

В этой части руководства разрабатываемое приложение использует флаг `X-KF-ReplyBack` для получения событий от Kaspersky CyberTrace без прослушивающего приложения. В части 2 этого руководства будет разработано приложение, прослушивающее события Kaspersky CyberTrace.

Флаг `X-KF-ReplyBack` включает режим ReplyBack mode. В этом режиме Kaspersky CyberTrace отправляет свои события обнаруженных киберугроз в то же самое сокетное соединение.

Этот флаг не является обязательным. Если приложение не отправит этот флаг, Kaspersky CyberTrace будет отправлять собственные события в соответствии с параметром OutputSettings > ConnectionString.

О флаге X-KF-SendFinishedEvent

Разрабатываемое приложение использует флаг `X-KF-SendFinishedEvent`, чтобы заставить Kaspersky CyberTrace генерировать специальное событие в ответ на каждое полученное событие.

Kaspersky CyberTrace генерирует это событие в формате, указанном в параметре OutputSettings > FinishedEventFormat. Значение атрибута `enabled` этого параметра игнорируется.

О флаге X-KF-SaveStatistic

Разрабатываемое приложение использует флаг `X-KF-SaveStatistic`, чтобы заставить Kaspersky CyberTrace сохранять статистику обнаружения киберугроз для всех событий, полученных при текущем подключении. События также сохраняются для ретроспективного сканирования.

1-й этап. Определение функции main()

На этом этапе выполняются следующие действия:

1. Импорт модуля `socket`.

   Функции из этого модуля используются для установления соединения с Kaspersky CyberTrace и отправки данных.

2. Определение функции `main()`.

3. В переменных `CYBERTRACE_ADDR` и `CYBERTRACE_PORT` необходимо указать адрес и порт, которые Kaspersky CyberTrace будет прослушивать в ожидании входящих событий.

   Эту информацию можно получить в веб-интерфейсе Kaspersky CyberTrace на странице General settings, в области **Входящие события**.

```
import socket

CYBERTRACE_ADDR = "192.0.2.42"
CYBERTRACE_PORT = 9999

def main():
    pass

if __name__ == '__main__':
    main()
```

2-й этап. Добавление примеров событий

На этом этапе выполняются следующие действия:

1. В функции `main()` определите список примеров событий.

События в этом списке содержат индикаторы. Приложение отправляет эти события в Kaspersky CyberTrace.

Каждое событие должно заканчиваться символом новой строки (`\n`). Символ новой строки служит разделителем событий.

```
def main():
    events = [
        '192.0.2.1\n',
        'ip=192.0.2.3\n',
        '776735A8CA96DB15B422879DA599F474\n',
        'EICAR md5=FEAF2058298C1E174C2B79AFFC7CF4DF\n',
        'Regular event\n',
        '44D88612FEA8A8F36DE82E1278ABB02F\n',
        'val1=04BFFABE7980E7D84424001896D2572E val2=0F9CCE3EA0EDFD6F41FF8A769F721631\n',
        'val=E9A6B1346D1A2447CABB980F3CC5DD27\n',
        'Regular event\n',
        'http://5a015004f9fc05290d87e86d69c4b237.com\n',
        'Domain: http://fakess123bn.nu\n',
    ]
```

3-й этап. Установление сокетного соединения

На этом этапе выполняются следующие действия:

1. В функцию `main()` необходимо добавить код, устанавливающий соединение с Kaspersky CyberTrace и завершающий соединение после отправки всех событий.

2. В этом коде необходимо отправить флаги `X-KF-SendFinishedEvent` и `X-KF-ReplyBack`.

   Флаги `X-KF-SendFinishedEvent` и `X-KF-ReplyBack` отправляются при установлении соединения. Эти флаги заставляют Kaspersky CyberTrace всегда генерировать событие в ответ на полученное событие, даже если при сопоставлении с полученного события с индикаторами не обнаруживается совпадений.

   Флаг `X-KF-SaveStatistic` следует отправлять, если требуется, чтобы в течение текущего соединения Kaspersky CyberTrace сохранял статистику обнаружения и события для ретроспективного сканирования (retroscan).

   Если используется флаг `X-KF-ReplyBack`, флаг `X-KF-SendFinishedEvent` должен ему предшествовать.

   Если используется флаг `X-KF-SaveStatistic`, флаг `X-KF-ReplyBack` должен ему предшествовать.

```
    ct_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    try:
        ct_socket.connect((CYBERTRACE_ADDR, CYBERTRACE_PORT))
        ct_socket.sendall(b'X-KF-SendFinishedEventX-KF-ReplyBackX-KF-SaveStatistic')
# Здесь будет код из следующего этапа
    finally:
        ct_socket.close()
```

4-й этап. Отправка событий

На этом этапе выполняются следующие действия:

1. В коде из предыдущего этапа в блоке `try... finally` выполняется итерация по списку `events` и каждое событие отправляется в Kaspersky CyberTrace.

Параметр `16384` в функции `socket.recv()` задает размер буфера сообщений. Если ожидается, что ответ будет содержать более 16384 байтов, увеличьте буфер. Это может потребоваться, если отдельные события содержат большое количество сопоставленных индикаторов.

```
        for event in events:
            ct_socket.sendall(event.encode())
            response = ct_socket.recv(16384)
```

2. Добавление вывода в консоль для отправленных событий и полученных ответов.

```
        for event in events:
            print("Sending:\n{}".format(event))
            ct_socket.sendall(event.encode())
            response = ct_socket.recv(16384)
            print("Response:\n{}".format(response.decode()))
```

5-й этап. Запуск приложения

На этом этапе выполняются следующие действия:

1. Запуск приложения из консоли:

```
python3 ./send_events_cybertrace.py
```

Ниже приведен пример вывода приложения. Kaspersky CyberTrace отправляет событие для каждого успешно сопоставленного индикатора и событие для завершенной операции поиска.

```
Sending:
val1=192.0.2.1 val2=ip=192.0.2.3

Response:
- category=KL_IP_Reputation matchedIndicator=192.0.2.1 url=- src=- ip=192.0.2.1 md5=- sha1=- sha256=- usrName=-
confidence=100 category=test first_seen=01.01.2017 00:00 ip=192.0.2.1 ip_geo=ru last_seen=16.07.2020 10:02
popularity=1 threat_score=75
- category=KL_IP_Reputation matchedIndicator=192.0.2.3 url=- src=- ip=192.0.2.3 md5=- sha1=- sha256=- usrName=-
confidence=100 category=test first_seen=15.01.2017 00:00 ip=192.0.2.3 ip_geo=ru last_seen=16.07.2020 09:51
popularity=1 threat_score=75
LookupFinished

Sending:
EICAR md5=FEAF2058298C1E174C2B79AFFC7CF4DF

Response:
- category=KL_Malicious_Hash_MD5 matchedIndicator=FEAF2058298C1E174C2B79AFFC7CF4DF url=- src=- ip=-
md5=FEAF2058298C1E174C2B79AFFC7CF4DF sha1=- sha256=- usrName=- confidence=100 MD5=FEAF2058298C1E174C2B79AFFC7CF4DF
SHA1=D01D17F6B13C7255A234F558ED85078EA5DD3F3D
SHA256=4CA914C9791CF2BF2AC69F9A2B21006F0361E247F2CE92F0A9F166DBC6B43670 file_size=1989 first_seen=10.07.2015 23:53
last_seen=13.07.2020 14:35 popularity=1 threat=HEUR:Trojan.Win32.Generic
LookupFinished

Sending:
Regular event

Response:
LookupFinished
```

Полный код для части 1

Ниже приведен полный код для части 1 этого руководства.

```
import socket

CYBERTRACE_ADDR = "192.0.2.42"
CYBERTRACE_PORT = 9999

def main():

    events = [
        '192.0.2.1\n',
        'ip=192.0.2.3\n',
        'val1=192.0.2.1 val2=ip=192.0.2.3\n',
        '776735A8CA96DB15B422879DA599F474\n',
        'EICAR md5=FEAF2058298C1E174C2B79AFFC7CF4DF\n',
        'Regular event\n',
        '44D88612FEA8A8F36DE82E1278ABB02F\n',
        'val1=04BFFABE7980E7D84424001896D2572E val2=0F9CCE3EA0EDFD6F41FF8A769F721631\n',
        'val=E9A6B1346D1A2447CABB980F3CC5DD27\n',
        'Regular event\n',
        'http://5a015004f9fc05290d87e86d69c4b237.com\n',
        'Domain: http://fakess123bn.nu\n',
    ]

    ct_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

    try:
        ct_socket.connect((CYBERTRACE_ADDR, CYBERTRACE_PORT))
        ct_socket.sendall(b'X-KF-SendFinishedEventX-KF-ReplyBackX-KF-SaveStatistic')

        for event in events:
            print("Sending:\n{}".format(event))
            ct_socket.sendall(event.encode())
            response = ct_socket.recv(16384)
            print("Response:\n{}".format(response.decode()))

    finally:
        ct_socket.close()


if __name__ == '__main__':

    main()
```

Учебное руководство по разработке приложения на Python: часть 2

В этом руководстве описывается реализация обмена данными с Kaspersky CyberTrace в приложении на Python.

В части 1 этого руководства описывается приложение, отправляющее данные в Kaspersky CyberTrace.

В части 2 этого руководства описывается приложение, ожидающее получения событий от Kaspersky CyberTrace.

Введение

Эта часть руководства посвящена реализации приложения Python, прослушивающего порт в ожидании событий от Kaspersky CyberTrace.

Имя для приложения можно выбрать произвольно. В примерах в этом руководстве для этого приложения используется имя файла `listen_events_cybertrace.py`.

О настройках подключения и форматах событий

Приложение будет прослушивать указанный адрес и порт, принимать входящие соединения от Kaspersky CyberTrace и выполнять парсинг полученных данных.

Для определения адреса и порта, на которые отправляются события, в Kaspersky CyberTrace используется параметр OutputSettings > ConnectionString. Адрес и порт для исходящих событий можно просмотреть и настроить на странице Service settings в веб-интерфейсе Kaspersky CyberTrace.

Для определения формата событий Kaspersky CyberTrace использует форматы из раздела OutputSettings конфигурационного файла Kaspersky CyberTrace Service. Каждое событие заканчивается символом новой строки (`\n`). Форматы событий можно настроить на странице Service alerts settings в веб-интерфейсе Kaspersky CyberTrace.

1-й этап. Определение функции main()

На этом этапе выполняются следующие действия:

1. Импорт модуля `socket`.

   Функции из этого модуля используются для установления соединения с Kaspersky CyberTrace и получения данных.

2. Определение функции `main()`.

3. В переменных `LISTEN_ADDR` и `LISTEN_PORT` необходимо указать адрес и порт, которые приложение будет прослушивать в ожидании входящих событий.

   Эту информацию можно получить в веб-интерфейсе Kaspersky CyberTrace на странице General settings, в области **Входящие события**.

```
import socket

LISTEN_ADDR = "192.0.2.105"
LISTEN_PORT = 9998

def main():
    pass
if __name__ == '__main__':
    main()
```

2-й этап. Добавление код сервера

На этом этапе выполняются следующие действия:

1. Добавление в функцию `main()` кода, запускающего сервер, прослушивающий указанные адрес и порт.

```
    server_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    print("Starting on {}:{}".format(LISTEN_ADDR, LISTEN_PORT))
    server_socket.bind((LISTEN_ADDR, LISTEN_PORT))
    server_socket.listen()
```

2. Добавление кода, обрабатывающего входящие соединения.

Функция `socket.accept()` принимает входящее соединение. Она возвращает новый объект сокета для соединения (в переменной `connection`) и адрес на другом конце, инициировавший соединение (в переменной `client_address`).

На этом этапе приложение игнорирует данные, полученные в результате соединений. Парсинг будет реализован на следующем этапе.

Приложение запускает бесконечный цикл. Его можно завершить стандартной комбинацией клавиш или командой операционной системы. В большинстве операционных систем это **^C** или **Ctrl+C**.

```
    while True:
        connection, client_address = server_socket.accept()
        try:
            print("Connection from {}".format(client_address))
            # Сюда добавляется парсинг данных
        finally:
            connection.close()
```

3-й этап. Парсинг полученных данных

На этом этапе выполняются следующие действия:

1. В блоке `try... finally` вызывается функцию, которая выполняет парсинг полученных данных на события.

   Поскольку в рамках каждого соединения может быть отправлено любое количество событий, приложение должно продолжать парсинг полученных данных, пока не будут обработаны все события. Функция `parse_response()` возвращает генератор. Затем этот генератор используется в цикле `for` для итерации по полученным событиям. На следующем шаге реализуется функция `parse_response()`.

   ```
        try:
            print("Connection from {}".format(client_address))
            for event in parse_response(connection):
                print("Received:\n{}".format(event.decode()))
        finally:
            connection.close()
   ```

2. Реализация функции `parse_response()`.

   События Kaspersky CyberTrace оканчиваются символом новой строки (`\n`). Функция `parse_response()` считывает данные из сокетного соединения в буфер до тех пор, пока в буфере не окажется символ новой строки. Затем функция выделяет событие из буфера и возвращает его. Функция `chunk_receive()` выполняет итерацию по данным из сокетного соединения. Эта функция будет реализована на следующем этапе.

   Когда цикл `for` из функции `main()` переходит к следующей итерации, функция `parse_response()` выделяет из буфера очередное событие и возвращает его. Если это невозможно, функция считывает дополнительные данные из соединения в буфер. Процесс повторяется до тех пор, пока из соединения не перестанут поступать данные и все события в буфере не будут возвращены.

   ```
   def parse_response(connection):
       buff = b''
       for data in chunk_receive(connection):
           buff += data
           while b'\n' in buff:
               event, buff = buff.split(b'\n',1)
               yield event
   ```

3. Реализация функции `chunk_receive()`.

   Функция `chunk_receive()` считывает 4096 байт данных из соединения и возвращает эти данные. Функция возвращает данные до тех пор, пока в соединении не закончатся данные.

Функция `socket.recv()` получает данные из соединения. Если данных нет, функция ожидает получения новых данных. При закрытии подключения функция возвращает ноль байтов, поэтому при выполнении этого условия цикл `while` завершается.

```
def chunk_receive(connection):
    data = None
    while data != b'':
        data = connection.recv(4096)
        yield data
```

Этап 5. (Необязательный) Изменение приложения, отправляющее события

Чтобы отправлять события в Kaspersky CyberTrace с помощью приложения, созданного в [части 1 этого руководства], измените его так, чтобы события отправлялись без ожидания ответа.

На этом этапе выполняются следующие действия:

1. Закомментируйте или удалите строку в коде приложения, которая отправляет флаги. Теперь Kaspersky CyberTrace отправляет события приложению-слушателю, поэтому флаг `X-KF-ReplyBack` становится излишним.

2. Закомментируйте или удалите строки, которые получают и выводят ответ.

Ниже приведен блок `try... finally` из приложения с закомментированными строками.

```
    try:
        ct_socket.connect((CYBERTRACE_ADDR, CYBERTRACE_PORT))
        #ct_socket.sendall(b'X-KF-SendFinishedEventX-KF-ReplyBack')

        for event in events:
            print("Sending:\n{}".format(event))
            ct_socket.sendall(event.encode())
            #response = ct_socket.recv(16384)
            #print("Response:\n{}".format(response.decode()))

    finally:
        ct_socket.close()
```

6-й этап. Запуск приложения

Запуск приложения из консоли:

```
python3 ./listen_events_cybertrace.py
```

Приложение прослушивает порт в ожидании событий обнаружения киберугроз и оповещений о событиях из Kaspersky CyberTrace и выводит их в консоль.

Если требуется отправлять события в Kaspersky CyberTrace с помощью приложения, разработанного в части 1 этого руководства, запустите это приложение из консоли:

```
python3 ./send_events_cybertrace.py
```

Ниже приведен пример вывода приложения.

```
Starting on 192.0.2.105:9998
Connection from ('192.0.2.42', 41882)
Received:
- category=KL_Malicious_Hash_MD5 matchedIndicator=776735A8CA96DB15B422879DA599F474 url=- src=- ip=-
md5=776735A8CA96DB15B422879DA599F474 sha1=- sha256=- usrName=- confidence=100 MD5=776735A8CA96DB15B422879DA599F474
SHA1=3B66A1D70562E291DA023E87B349DD89DFE00213
SHA256=1963CBCBB9FDAAD45F782FAAA467EE2C115C3111C003AE14D01181880B03F6ED file_size=1431 first_seen=10.07.2015 23:53
last_seen=14.07.2020 13:35 popularity=1 threat=HEUR:Trojan.Win32.Generic
Received:
- category=KL_IP_Reputation matchedIndicator=192.0.2.1 url=- src=- ip=192.0.2.1 md5=- sha1=- sha256=- usrName=-
confidence=100 category=test first_seen=01.01.2017 00:00 ip=192.0.2.1 ip_geo=ru last_seen=17.07.2020 09:02
popularity=1 threat_score=75
Received:
- category=KL_Malicious_Hash_MD5 matchedIndicator=FEAF2058298C1E174C2B79AFFC7CF4DF url=- src=- ip=-
md5=FEAF2058298C1E174C2B79AFFC7CF4DF sha1=- sha256=- usrName=- confidence=100 MD5=FEAF2058298C1E174C2B79AFFC7CF4DF
SHA1=D01D17F6B13C7255A234F558ED85078EA5DD3F3D
SHA256=4CA914C9791CF2BF2AC69F9A2B21006F0361E247F2CE92F0A9F166DBC6B43670 file_size=1989 first_seen=10.07.2015 23:53
last_seen=14.07.2020 13:35 popularity=1 threat=HEUR:Trojan.Win32.Generic
Received:
- category=KL_IP_Reputation matchedIndicator=192.0.2.3 url=- src=- ip=192.0.2.3 md5=- sha1=- sha256=- usrName=-
confidence=100 category=test first_seen=15.01.2017 00:00 ip=192.0.2.3 ip_geo=ru last_seen=17.07.2020 08:51
popularity=1 threat_score=75
```

Полный код для части 2

Ниже приведен полный код для части 2 этого руководства.

```
import socket

LISTEN_ADDR = "192.0.2.105"
LISTEN_PORT = 9998

def chunk_receive(connection):
    data = None
    while data != b'':
        data = connection.recv(4096)
        yield data

def parse_response(connection):
    buff = b''
    for data in chunk_receive(connection):
        buff += data
        while b'\n' in buff:
            event, buff = buff.split(b'\n',1)
            yield event

def main():

    server_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    print("Starting on {}:{}".format(LISTEN_ADDR, LISTEN_PORT))
    server_socket.bind((LISTEN_ADDR, LISTEN_PORT))
    server_socket.listen()

    while True:
        connection, client_address = server_socket.accept()
        try:
            print("Connection from {}".format(client_address))
            for event in parse_response(connection):
                print("Received:\n{}".format(event.decode()))
        finally:
            connection.close()

if __name__ == '__main__':

    main()
```

Справочник по REST API

В этой главе представлена информация об использовании REST API Kaspersky CyberTrace.

О REST API

В этом разделе описываются возможности REST API Kaspersky CyberTrace.

О REST API

Kaspersky CyberTrace предоставляет интерфейс REST API, с помощью которого можно выполнять следующие действия:

- Выполнение поиска индикаторов.
- Выполнение поиска индикаторов в пределах определенного тенанта.
- Добавление новых источников данных об угрозах, а также настройка и удаление источников данных об угрозах, которые были добавлены с помощью REST API.
- Добавление, удаление и обновление индикаторов источников данных об угрозах для источников данных об угрозах, которые были добавлены с помощью REST API, а также для источников данных об угрозах *InternalTI* и *FalsePositive*.
- Добавление, удаление и обновление индикаторов источников данных об угрозах в рамках определенного тенанта.
- Обновление и получение информации об источнике данных об угрозах в рамках определенного тенанта.
- Добавление, обновление и удаление тегов в базе данных Kaspersky CyberTrace. Назначение тегов индикаторам и снятие тегов с индикаторов.

Поддерживаемые протоколы

REST API поддерживает протокол HTTPS с базовой аутентификацией. Все запросы синхронные. Kaspersky CyberTrace обрабатывает запрос и возвращает результат в ответе.

Для обмена данными по протоколу HTTPS Kaspersky CyberTrace использует сертификат, указанный в элементах `ServiceSettings → HTTPServer → SSLCertificatePath` и `ServiceSettings → HTTPServer → SSLPrivateKeyPath` конфигурационного файла kl_feed_service.conf.

Максимальное количество обрабатываемых запросов задается в элементе `ServiceSettings → ScannersCount` конфигурационного файла kl_feed_service.conf.

Источники данных об угрозах REST API

Источники данных об угрозах, добавленные с помощью REST API, отличаются от обычных источников данных об угрозах. Посредством REST API можно работать только с теми источниками данных об угрозах, которые были добавлены через REST API. Обращаться через REST API ко всем остальным источникам данных об угрозах невозможно. Кроме того, REST API предоставляет возможность управления индикаторами из источников данных об угрозах *FalsePositive* и *InternalTI*.

Источники данных об угрозах, добавленные с помощью REST API, отображаются на вкладке «Custom feeds». Если для источника данных об угрозах указан поставщик, такой источник данных об угрозах отображается на вкладке поставщика. У каждого источника данных об угрозах REST API есть краткое описание, в котором он обозначен как источник данных об угрозах REST API.

Для источников данных об угрозах которые были добавлены с помощью REST API невозможно выполнять следующие действия в веб-интерфейсе Kaspersky CyberTrace:

- Редактирование свойств источника данных об угрозах.
- Включение или отключение полей источника данных об угрозах.
- Определение правил фильтрации для источника данных об угрозах.
- Указание максимального количества записей в источнике данных об угрозах.

В веб-интерфейсе Kaspersky CyberTrace можно выполнять следующие действия с источниками данных об угрозах, которые были добавлены с помощью REST API:

- Указание полей контекста для источника данных об угрозах.
- Включение или выключение источника данных об угрозах.
- Удаление источника данных об угрозах.

Роли пользователей и REST API

Доступные пользователю методы зависят от роли пользователя:

- Пользователи с ролью «Администратор» могут выполнять все запросы.
- Пользователи с ролью «Аналитик» могут выполнять поиск индикаторов.
- Пользователи с ролью «Менеджер тенанта» могут выполнять определенные запросы с указанием имени тенанта.

REST API и ведение журнала

Kaspersky CyberTrace заносит в журнал следующую информацию о REST API:

- Если уровень ведения журнала — *err* и выше, Kaspersky CyberTrace регистрирует информацию об ошибках REST API.
- Если уровень ведения журнала — *info* и выше, Kaspersky CyberTrace регистрирует информацию обо всех запросах и ответах REST API.

Доступ к REST API

В этом разделе описывается порядок получения доступа к REST API Kaspersky CyberTrace.

Конечная точка REST API

Kaspersky CyberTrace принимает запросы на конечной точке, состоящей из IP-адреса сервера с Kaspersky CyberTrace и порта, указанного в `элементе ServiceSettings → HTTPServer → ConnectionString` конфигурационного файла kl_feed_service.conf.

Используется следующий формат адреса:

```
https://%ENDPOINT%/api/%API_VERSION%/%REQUEST%
```

Например, если `ConnectionString` — `0.0.0.0:104`, а IP-адрес сервера с Kaspersky CyberTrace — 192.168.0.2, поисковый запрос должен направляться на следующий адрес:

```
https://192.168.0.2:104/api/1.1/lookup
```

Заголовки запроса

Каждый запрос должен иметь следующие заголовки:

- Accept

  Тип содержимого ответа. Этот заголовок должен иметь значение `application/json`.

- Authorization

  Этот заголовок должен содержать строку базовой авторизации.

Базовая авторизация

Учетные данные для базовой схемы авторизации строятся следующим образом:

1. Имя пользователя и пароль объединяются двоеточием.

   Например, если имя пользователя — `user`, а пароль — `password`, формируется строка `user:password`.

2. Полученная строка затем кодируется в base64.

   В приведенном выше примере получается строка `dXNlcjpwYXNzd29yZA==`.

3. Окончательная строка авторизации создается путем добавления строки "Basic" в начало строки учетных данных.

   В приведенном выше примере окончательной строкой авторизации будет `Basic dXNlcjpwYXNzd29yZA==`.

Статусы ответов

В этом разделе описываются статусы ответов REST API Kaspersky CyberTrace.

Дополнительные сведения об ответах приведены в описаниях отдельных запросов.

200 OK

Этот статус возвращается в ответ на успешно обработанные запросы. В теле ответа содержится результат.

201 Created

Этот статус возвращается, если сущность (источник данных об угрозах или индикатор) была успешно создана. В теле ответа содержится статус операции.

202 Partial success

Этот статус возвращается, если успешно создано было только подмножество сущностей (индикаторов). В теле ответа содержится статус операции и информация о сущностях, которые не были обработаны.

401 Unauthorized user

Пользователь не авторизован, указанный пользователь не существует или пароль, указанный в заголовке Authorization, недействителен.

Примеры:

- Запрос без заголовка *Authorization* возвращает этот статус.
- Этот статус возвращается в ответ на запрос с попыткой авторизации несуществующей учетной записи пользователя.

403 User does not have rights to this operation

У пользователя нет прав на выполнение операции. Это может иметь место, например, когда текущая лицензия не распространяется на поиск индикаторов или когда добавить индикаторы или новый источник данных об угрозах пытается пользователь с ролью «Аналитик».

В теле ответа может содержаться описание ошибки.

404 Request not supported

Указанный запрос или версия API не поддерживаются.

Примеры:

- Запрос *login* не поддерживается. Этот статус возвращает запрос `POST /api/1.0/login`.
- Версия API 8.0 не поддерживается. Этот статус возвращает запрос `POST /api/8.0/lookup`.

405 Method Not Allowed

Указанный метод не поддерживается.

Например, запрос *lookup* поддерживает только метод POST. Этот статус возвращает запрос `GET /api/1.1/lookup`.

425 Kaspersky CyberTrace initializing

Запрос был сделан до завершения инициализации Kaspersky CyberTrace.

406 Not Acceptable

Указанный формат данных не поддерживается.

Например, если заголовок Accept содержит значение application/pdf, в ответ возвращается этот статус.

429 Too Many Requests

Kaspersky CyberTrace не может обработать запрос.

Запрос отклонен и не обрабатывается. Необходимо будет сделать еще один запрос позже.

400 Bad Request

Запрос имеет неверный формат:

- В запросе отсутствуют какие-либо из обязательных заголовков.
- Необходимо тело запроса, но его нет.
- Тело запроса имеет неверный формат.
- Параметры тела запроса имеют недопустимые значения.
- Размер тела запроса не соответствует требованиям.

500 Internal Server Error

При обработке запроса произошла ошибка

В теле ответа может содержаться описание ошибки.

Запросы

В этом разделе описываются запросы, которые можно выполнять с помощью API Kaspersky CyberTrace, ответы на данные запросы и примеры использования.

Начиная с версии 5.0, Kaspersky CyberTrace поддерживает три версии REST API: 1.0, 1.1, 1.2 и 1.3.

Если ваш лицензионный ключ поддерживает мультитенантность, в каждом запросе должен быть указан тенант, для которого выполняется запрос.

В следующей таблице перечислены запросы, доступные для каждой версии.

Запросы REST API

Запрос	REST API v1.0	REST API версий 1.1 и 1.2	REST API 1.3
`POST /api/%API_VERSION%/lookup` Выполнение поиска индикаторов.	Да	Да	Нет
`POST /api/%API_VERSION%/{TenantName}/lookup` Выполняет поиск по индикатору в указанном тенанте.	Нет	Нет	Да Доступно, толь если включен режим мультитенантно
Управление источниками данных об угрозах			
`GET /api/%API_VERSION%/suppliers` Получение списка источников данных об угрозах и их статусов.	Да	Да	Да
`POST /api/%API_VERSION%/suppliers` Добавление нового источника данных об угрозах.	Да	Да	Да
`GET /api/%API_VERSION%/suppliers/{supplier}` Получение информации об указанном источнике данных об угрозах.	Да	Да	Да
`GET /api/%API_VERSION%/{TenantName}/suppliers/{supplier}` Получение информации об указанном источнике данных об угрозах в рамках указанного тенанта.	Нет	Нет	Да Доступно, толь если включен режим мультитенантно
`PUT /api/%API_VERSION%/suppliers/{supplier}` Обновление указанной информации об источнике данных об угрозах.	Да	Да	Да
`PUT /api/%API_VERSION%/{TenantName}/suppliers/{supplier}` Обновление указанной информации об источнике данных об угрозах в рамках указанного тенанта.	Нет	Нет	Да Доступно, толь если включен режим мультитенантно
`DELETE /api/%API_VERSION%/suppliers/{supplier}` Удаление указанного источника данных об угрозах.	Да	Да	Да
Управление индикаторами			
`PUT /api/%API_VERSION%/suppliers/{supplier}/indicators` Добавление в источник данных об угрозах новых индикаторов и обновление существующих индикаторов.	Да Добавление тегов к индикаторам или снятие тегов с индикаторов недоступно.	Да Начиная с версии 1.2, приложение поддерживает возможность отмечать связанные с индикаторами обнаруженные киберугрозы как ложные срабатывания.	Да
`PUT /api/%API_VERSION%/{TenantName}/suppliers/{supplier}/indicators` Добавление в источник данных об угрозах новых индикаторов и обновление существующих индикаторов в рамках указанного тенанта.	Нет	Нет	Да Доступно, толь если включен режим мультитенантно

Запрос	REST API v1.0	REST API версий 1.1 и 1.2	REST API 1.3
`DELETE /api/%API_VERSION%/suppliers/{supplier}/indicators` Удаление указанных индикаторов из источника данных об угрозах.	Да	Да Начиная с версии 1.2, приложение поддерживает возможность удалять связанные с индикаторами обнаруженные киберугрозы из списка ложных срабатываний.	Да
`DELETE /api/%API_VERSION%/{TenantName}/suppliers/{supplier}/indicators` Удаление указанных индикаторов из источника данных об угрозах в рамках указанного тенанта.	Нет	Нет	Да Доступно, толь если включен режим мультитенантно
`PUT /api/%API_VERSION%/{TenantName}/settings/publicApi` Позволяет сохранять обнаружения индикаторов, полученных через общедоступные API.	Нет	Нет	Да
`GET /api/%API_VERSION%/{TenantName}/settings/publicApi` Получает от тенанта статус функции сохранения обнаружений индикаторов, полученных через общедоступные API.	Нет	Нет	Да
Работа с тегами			
`GET /api/%API_VERSION%/tags` Получение списка тегов.	Нет	Да	Да
`POST /api/%API_VERSION%/tags` Добавление нового тега.	Нет	Да	Да
`GET /api/%API_VERSION%/tags/{tag}` Получение информации об указанном теге.	Нет	Да	Да
`PUT /api/%API_VERSION%/tags/{tag}` Обновление указанного тега.	Нет	Да	Да
`DELETE /api/%API_VERSION%/tags/{tag}` Удаление указанного тега.	Нет	Да	Да

POST lookup

Выполнение поиска индикатора.

Путь

`/api/%API_VERSION%/lookup`

Метод

`POST`

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.
`Content-Type`	`application/json`	Тип содержимого запроса. Также можно указать кодировку `utf-8`. Например: `Content-Type: application/json; charset=utf-8`
`Content-Length`	Integer	Размер тела запроса в байтах. Максимальный размер тела этого запроса составляет 64 МБ (`67108864`).

Тело запроса

Тело этого запроса содержит массив объектов для поиска в формате JSON. Должен быть указан хотя бы один объект.

```
[{"object":"%OBJECT_VALUE%"},...{"object":"%OBJECT_VALUE%"}]
```

Свойства объекта описаны в следующей таблице.

Свойства объекта

Свойство	Значение	Обязательное	Описание
`object`	String	Да	Объект для поиска.

Пример запроса

Ниже приведен пример запроса *POST lookup*.

```
POST https://192.168.2.57/api/1.1/lookup

Accept: application/json
Content-Type: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
Content-Length: 81

[{"object":"http:\/\/example.com"},{"object":"C1153422C5F68E731347F6A33F791598"}]
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит массив объектов результатов поиска в формате JSON.

```
[
    {
     "object": "%OBJECT_VALUE%",
     "result": "%LOOKUP_RESULT%",
     "categories":
        [
            {
             "category": "%CATEGORY_1%",
             "detected_indicator": "%DETECTED_INDICATOR%",
             "context":
                {
                    "%supplier_field_1%": "%supplier_field_1_value%",
                    ...
                    "%supplier_field_N%": "%supplier_field_N_value%"
                }
            },
            ...
            {
             "category": "%CATEGORY_N%",
             "detected_indicator": "%DETECTED_INDICATOR%",
             "context":
                {
                    "%supplier_field_1%": "%supplier_field_1_value%",
                    ...
                    "%supplier_field_N%": "%supplier_field_N_value%"
                }
            }
        ]
    },
    ...
    {
     "object": "%OBJECT_VALUE%",
     "result": "%LOOKUP_RESULT%",
     "categories":
        [
            {
             "category": "%CATEGORY_1%",
             "detected_indicator": "%DETECTED_INDICATOR%",
```

```
            "context":
               {
                   "%supplier_field_1%": "%supplier_field_1_value%",
                   ...
               }
           },
           ...
        ]
    }
]
```

Свойства объекта результатов поиска описаны в следующей таблице.

Свойства объекта результатов поиска

Свойство	Значение	Описание
`object`	String	Объект, поиск которого выполнялся.
`result`	String	Результат поиска. Возможны следующие значения: • *detected* Обнаружено совпадение с индикаторами. • *not detected* Совпадений с индикаторами не обнаружено. • *error* Произошла ошибка во время поиска.
`categories`	Array	Массив объектов категорий, см. описание ниже. Это свойство включается, если *result* имеет значение «`detected`».
`reason`	Строка	Причина ошибки.

Свойства объектов категории описаны в следующей таблице.

Свойства объекта категории

Свойство	Значение	Описание
`category`	Строка	Категория обнаружения киберугрозы.
`detected_indicator`	Строка	Сопоставленный индикатор.
`context`	Array	Массив объектов контекста.

Свойства объектов контекста описаны в следующей таблице.

Свойства объекта контекста

Свойство	Значение	Описание
`%field_name%`	Строка	Имя свойства соответствует имени одного из полей сопоставленного индикатора. Значение свойства содержит значение поля.

Пример ответа

Ниже приведен пример ответа на запрос *POST lookup*.

```
HTTP/1.1 200 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 372

[{"object":"http:\/\/example.com","result":"not detected"},
 {"object":"C1153422C5F68E731347F6A33F791598","result":"detected", "detects":
    [{"category":"KL_Malicious_Hash","detected_indicator":"C1153422C5F68E731347F6A33F791598","context":
{"first_seen":"10.07.2015 23:53","threat":"Trojan.Win32.Generic"}}]}
]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
    {
        "status": "%ERROR%"
    }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.
`reason`	Строка	Причина ошибки.

Пример ошибочного ответа

Ниже приведен пример ответа с ошибкой на запрос *POST lookup*.

```
HTTP/1.1 500 Internal Server Error
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 75

[{"status": "An error occurred while creating supplier", "reason": "Supplier already exists"}]
```

POST lookup (режим мультитенантности)

Выполняет поиск по индикатору в указанном тенанте.

Путь

`/api/%API_VERSION%/{TenantName}/lookup`

Метод

`POST`

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.
`Content-Type`	`application/json`	Тип содержимого запроса. Также можно указать кодировку `utf-8`. Например: `Content-Type: application/json; charset=utf-8`
`Content-Length`	Integer	Размер тела запроса в байтах. Максимальный размер тела этого запроса составляет 64 МБ (`67108864`).

Тело запроса

Тело этого запроса содержит массив объектов для поиска в формате JSON. Должен быть указан хотя бы один объект.

```
[{"object":"%OBJECT_VALUE%"},...{"object":"%OBJECT_VALUE%"}]
```

Свойства объекта описаны в следующей таблице.

Свойства объекта

Свойство	Значение	Обязательное	Описание
`object`	String	Да	Объект для поиска.

Пример запроса

Ниже приведен пример запроса *POST lookup*.

```
POST https://192.168.2.57/api/1.3/ExampleTenant/lookup

Accept: application/json
Content-Type: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
Content-Length: 81

[{"object":"http:\/\/example.com"},{"object":"C1153422C5F68E731347F6A33F791598"}]
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит массив объектов результатов поиска в формате JSON.

```
[
    {
     "object": "%OBJECT_VALUE%",
     "result": "%LOOKUP_RESULT%",
     "categories":
        [
            {
             "category": "%CATEGORY_1%",
             "detected_indicator": "%DETECTED_INDICATOR%",
             "context":
                {
                    "%supplier_field_1%": "%supplier_field_1_value%",
                    ...
                    "%supplier_field_N%": "%supplier_field_N_value%"
                }
            },
            ...
            {
             "category": "%CATEGORY_N%",
             "detected_indicator": "%DETECTED_INDICATOR%",
             "context":
                {
                    "%supplier_field_1%": "%supplier_field_1_value%",
                    ...
                    "%supplier_field_N%": "%supplier_field_N_value%"
                }
            }
        ]
    },
    ...
```

```
    {
     "object": "%OBJECT_VALUE%",
     "result": "%LOOKUP_RESULT%",
     "categories":
        [
            {
             "category": "%CATEGORY_1%",
             "detected_indicator": "%DETECTED_INDICATOR%",
             "context":
                {
                    "%supplier_field_1%": "%supplier_field_1_value%",
                    ...
                }
            },
            ...
        ]
    }
]
```

Свойства объекта результатов поиска описаны в следующей таблице.

Свойства объекта результатов поиска

Свойство	Значение	Описание
`object`	String	Объект, поиск которого выполнялся.
`result`	String	Результат поиска. Возможны следующие значения: • *detected* Обнаружено совпадение с индикаторами. • *not detected* Совпадений с индикаторами не обнаружено. • *error* Произошла ошибка во время поиска.
`categories`	Array	Массив объектов категорий, см. описание ниже. Это свойство включается, если *result* имеет значение «`detected`».
`reason`	Строка	Причина ошибки.

Свойства объектов категории описаны в следующей таблице.

Свойства объекта категории

Свойство	Значение	Описание
`category`	Строка	Категория обнаружения киберугрозы.
`detected_indicator`	Строка	Сопоставленный индикатор.
`context`	Array	Массив объектов контекста.

Свойства объектов контекста описаны в следующей таблице.

Свойства объекта контекста

Свойство	Значение	Описание
`%field_name%`	Строка	Имя свойства соответствует имени одного из полей сопоставленного индикатора. Значение свойства содержит значение поля.

Пример ответа

Ниже приведен пример ответа на запрос *POST lookup*.

```
HTTP/1.3 200 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 372

[{"object":"http:\/\/example.com","result":"not detected"},
 {"object":"C1153422C5F68E731347F6A33F791598","result":"detected", "detects":
    [{"category":"KL_Malicious_Hash","detected_indicator":"C1153422C5F68E731347F6A33F791598","context":
{"first_seen":"10.07.2015 23:53","threat":"Trojan.Win32.Generic"}}]}
]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
    {
        "status": "%ERROR%"
    }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.
`reason`	Строка	Причина ошибки.

Пример ошибочного ответа

Ниже приведен пример ответа с ошибкой на запрос *POST lookup*.

```
HTTP/1.3 500 Internal Server Error
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 75

[{"status": "An error occurred while creating supplier", "reason": "Supplier already exists"}]
```

GET suppliers

Получение списка источников данных об угрозах и их статусов.

Возвращаются только источники данных об угрозах, созданные с помощью REST API, а также источники данных об угрозах *FalsePositive* и *InternalTI*.

Путь

`/api/%API_VERSION%/suppliers`

Метод

`GET`

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.

Тело запроса

Тело этого запроса пустое.

Пример запроса

Ниже приведен пример запроса *GET suppliers*.

```
GET https://192.168.2.57/api/1.1/suppliers

Accept: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит массив объектов статуса источников данных об угрозах в формате JSON.

```
[
    {
      "name":"%SUPPLIER_NAME_1%",
      "status": "%SUPPLIER_STATUS%"
    },
...
    {
      "name":"%SUPPLIER_NAME_N%",
      "status": "%SUPPLIER_STATUS%"
    }
]
```

Описание свойств объекта статуса источника данных об угрозах приведено в следующей таблице.

Свойства объекта статуса источника данных об угрозах

Свойство	Значение	Описание
`name`	Строка	Имя источника данных об угрозах.
`status`	Строка	Статус источника данных об угрозах. Значение `enabled`, если источник данных об угрозах включен. Значение `disabled`, если источник данных об угрозах отключен.

Пример ответа

Ниже приведен пример ответа на запрос *GET suppliers*.

```
HTTP/1.1 200 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 99

[
 {"name":"ExampleSupplier", "status":"enabled"}, {"name":"AnotherExampleSupplier", "status":"disabled"}
]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
    {
        "status": "An error occurred while getting a list of suppliers",
    }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.

Пример ошибочного ответа

Ниже приведен пример ответа с ошибкой на запрос *GET suppliers*.

```
HTTP/1.1 500 Internal Server Error
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 63

[{"status": "An error occurred while getting a list of suppliers"}]
```

POST suppliers

Добавление нового источника данных об угрозах.

Добавленный источник данных об угрозах является источником данных об угрозах REST API, и им можно управлять с помощью методов REST API. Новый источник данных об угрозах включен по умолчанию.

Путь

`/api/%API_VERSION%/suppliers`

Метод

`POST`

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.
`Content-Type`	`application/json`	Тип содержимого запроса. Также можно указать кодировку `utf-8`. Например: `Content-Type: application/json; charset=utf-8`
`Content-Length`	Integer	Размер тела запроса в байтах. Максимальный размер тела этого запроса составляет 128 МБ (`134217728`).

Тело запроса

Тело этого запроса содержит массив JSON с объектом источника данных об угрозах. Должен быть указан только один объект источника данных об угрозах.

```
[
    {
      "name":"%SUPPLIER_NAME%",
      "confidence": %SUPPLIER_CONFIDENCE%,
      "retention": %SUPPLIER_RETENTION%,
      "vendor": "%SUPPLIER_VENDOR%"
    }
]
```

Свойства объекта источника данных об угрозах описаны в следующей таблице.

Свойства объекта источника данных об угрозах

Свойство	Значение	Обязательное	Описание
`name`	Строка	Да	Имя источника данных об угрозах. Имя источника данных об угрозах должно содержать только латинские буквы, цифры, дефисы («-») и символы подчеркивания («_»). В имени источника данных об угрозах не допускаются символы пробела (« »). В качестве имени источника данных об угрозах не следует использовать *FalsePositive* или *InternalTI*, поскольку эти имена зарезервированы для встроенных источников данных об угрозах Kaspersky CyberTrace.
`confidence`	Целое число	Да	Уровень доверия к индикаторам из этого источника данных об угрозах. Диапазон значений этого параметра: от `0` до `100`.
`retention`	Целое число	Да	Срок хранения индикаторов в минутах. Этот параметр определяет время ожидания, по истечении которого индикаторы этого источника данных об угрозах перестают использоваться в сопоставлении. Этот период времени отсчитывается с момента последнего обновления индикатора.
`vendor`	Строка	Нет	Имя поставщика источника данных об угрозах.

Пример запроса

Ниже приведен пример запроса *POST suppliers*.

```
POST https://192.168.2.57/api/1.1/suppliers

Accept: application/json
Content-Type: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
Content-Length: 91
[
 {"name":"ExampleSupplier", "confidence": 90, "retention": 5000, "vendor": "ExampleVendor"}
]
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит объект JSON со статусом операции.

```
[
    {
        "status": "Supplier successfully created"
    }
]
```

Свойства объекта статуса описаны в следующей таблице.

Свойства объекта статуса

Свойство	Значение	Описание
`status`	Строка	Статус операции.

Пример ответа

Ниже приведен пример ответа на запрос *POST suppliers*.

```
HTTP/1.1 201 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 41

[{"status": "Supplier successfully created"}]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
    {
        "status": "An error occurred while creating some suppliers",
        "reason": "%REASON%"
    }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.
`reason`	Строка	Причина ошибки.

Пример ошибочного ответа

Ниже приведен пример ответа с ошибкой на запрос *POST suppliers*.

```
HTTP/1.1 400 Bad Request
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 92

[{"status": "An error occurred while creating some suppliers", "reason": "Incorrect supplier name"}]
```

GET suppliers/{supplier}

Получение информации об указанном источнике данных об угрозах.

Возвращаются только источники данных об угрозах, созданные с помощью REST API, а также источники данных об угрозах *FalsePositive* и *InternalTI*.

Путь

```
/api/%API_VERSION%/suppliers/{supplier}
```

Метод

`GET`

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.

Параметры запроса

Этот запрос имеет следующие параметры:

Параметры запроса

Имя	Тип параметра	Описание
`supplier`	Путь	Имя источника данных об угрозах.

Тело запроса

Тело этого запроса пустое.

Пример запроса

Ниже приведен пример запроса *GET suppliers/{supplier}*.

```
GET https://192.168.2.57/api/1.1/suppliers/ExampleSupplier

Accept: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит массив JSON с объектом информации об источнике данных об угрозах.

```
[
    {
      "name": "%SUPPLIER_NAME%",
      "status": "%SUPPLIER_STATUS%",
      "confidence": %SUPPLIER_CONFIDENCE%,
      "retention": %SUPPLIER_RETENTION%,
      "vendor": "%SUPPLIER_VENDOR%"
    }
]
```

Свойства объекта информации об источники данных об угрозах описаны в следующей таблице.

Свойства объекта информации об источнике данных об угрозах

Свойство	Значение	Описание
`name`	Строка	Имя источника данных об угрозах.
`status`	Строка	Статус источника данных об угрозах. Значение `enabled`, если источник данных об угрозах включен. Значение `disabled`, если источник данных об угрозах отключен.
`confidence`	Целое число	Уровень доверия к индикаторам из этого источника данных об угрозах.
`retention`	Целое число	Срок хранения индикаторов в минутах.
`vendor`	Строка	Имя поставщика источника данных об угрозах.

Пример ответа

Ниже приведен пример ответа на запрос *GET suppliers/{supplier}*.

```
HTTP/1.1 200 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 108

[
 {name:"ExampleSupplier", "status":"enabled", "confidence": 90, "retention": 5000, "vendor": "ExampleVendor"}
]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
    {
        "status": "Supplier doesn't exist",
    }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.

Пример ошибочного ответа

Ниже приведен пример ответа с ошибкой на запрос *GET suppliers/{supplier}*.

```
HTTP/1.1 404 Supplier doesn't exist
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 34

[{"status": "Supplier doesn't exist"}]
```

GET suppliers/{supplier} (режим мультитенантности)

Получение информации об указанном источнике данных об угрозах в рамках указанного тенанта.

Возвращаются только источники данных об угрозах, созданные с помощью REST API, а также источники данных об угрозах *FalsePositive* и *InternalTI*.

Путь

`/api/%API_VERSION%/{TenantName}/suppliers/{supplier}`

Метод

`GET`

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.

Параметры запроса

Этот запрос имеет следующие параметры:

Параметры запроса

Имя	Тип параметра	Описание
`supplier`	Путь	Имя источника данных об угрозах.

Тело запроса

Тело этого запроса пустое.

Пример запроса

Ниже приведен пример запроса *GET suppliers/{supplier}*.

```
GET https://192.168.2.57/api/1.3/ExampleTenant/suppliers/ExampleSupplier

Accept: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит массив JSON с объектом информации об источнике данных об угрозах.

```
[
    {
      "name": "%SUPPLIER_NAME%",
      "status": "%SUPPLIER_STATUS%",
      "confidence": %SUPPLIER_CONFIDENCE%,
      "retention": %SUPPLIER_RETENTION%,
      "vendor": "%SUPPLIER_VENDOR%"
    }
]
```

Свойства объекта информации об источники данных об угрозах описаны в следующей таблице.

Свойства объекта информации об источнике данных об угрозах

Свойство	Значение	Описание
`name`	Строка	Имя источника данных об угрозах.
`status`	Строка	Статус источника данных об угрозах. Значение `enabled`, если источник данных об угрозах включен. Значение `disabled`, если источник данных об угрозах отключен.
`confidence`	Целое число	Уровень доверия к индикаторам из этого источника данных об угрозах.
`retention`	Целое число	Срок хранения индикаторов в минутах.
`vendor`	Строка	Имя поставщика источника данных об угрозах.

Пример ответа

Ниже приведен пример ответа на запрос *GET suppliers/{supplier}*.

```
HTTP/1.3 200 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 108

[
 {name:"ExampleSupplier", "status":"enabled", "confidence": 90, "retention": 5000, "vendor": "ExampleVendor"}
]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
    {
        "status": "Supplier doesn't exist",
```

```
    }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.

Пример ошибочного ответа

Ниже приведен пример ответа с ошибкой на запрос *GET suppliers/{supplier}*.

```
HTTP/1.3 404 Supplier doesn't exist
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 34

[{"status": "Supplier doesn't exist"}]
```

PUT suppliers/{supplier}

Обновление указанной информации об источнике данных об угрозах.

С помощью этого запроса могут обновляться только источники данных об угрозах, созданные с помощью REST API.

Путь

`/api/%API_VERSION%/suppliers/{supplier}`

Метод

`PUT`

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.
`Content-Type`	`application/json`	Тип содержимого запроса. Также можно указать кодировку `utf-8`. Например: `Content-Type: application/json; charset=utf-8`
`Content-Length`	Integer	Размер тела запроса в байтах. Максимальный размер тела этого запроса составляет 128 МБ (`134217728`).

Параметры запроса

Этот запрос имеет следующие параметры:

Параметры запроса

Имя	Тип параметра	Описание
`supplier`	Путь	Имя источника данных об угрозах.

Тело запроса

Тело этого запроса содержит массив JSON с объектом источника данных об угрозах. Должен быть указан только один объект источника данных об угрозах.

```
[
    {
      "name":"%SUPPLIER_NAME%",
      "status":"%SUPPLIER_STATUS%",
      "confidence": %SUPPLIER_CONFIDENCE%,
      "retention": %SUPPLIER_RETENTION%,
      "vendor": "%SUPPLIER_VENDOR%"
    }
]
```

Свойства объекта источника данных об угрозах описаны в следующей таблице.

Свойства объекта источника данных об угрозах

Свойство	Значение	Обязательное	Описание
`name`	Строка	Нет	Имя источника данных об угрозах.
`status`	Строка	Нет	Статус источника данных об угрозах. Если источник данных об угрозах требуется включить, значение должно быть `enabled`. Если источник данных об угрозах требуется отключить, значение должно быть `disabled`.
`confidence`	Целое число	Нет	Уровень доверия к индикаторам из этого источника данных об угрозах.
`retention`	Целое число	Нет	Срок хранения индикаторов в минутах. Этот параметр определяет период, по истечении которого индикаторы этого источника данных об угрозах перестают использоваться в сопоставлении.
`vendor`	Строка	Нет	Имя поставщика источника данных об угрозах.

Пример запроса

Ниже приведен пример запроса *PUT suppliers/{supplier}*.

```
PUT https://192.168.2.57/api/1.1/suppliers/ExampleSupplier

Accept: application/json
Content-Type: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
Content-Length: 41

[
 {"name":"NewName", "confidence": 90}
]
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит объект JSON со статусом операции.

```
[
    {
        "status": "Supplier info successfully updated"
    }
]
```

Свойства объекта статуса описаны в следующей таблице.

Свойства объекта статуса

Свойство	Значение	Описание
`status`	Строка	Статус операции.

Пример ответа

Ниже приведен пример ответа на запрос *PUT suppliers/{supplier}*.

```
HTTP/1.1 201 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 46

[{"status": "Supplier info successfully updated"}]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
    {
        "status": "An error occurred while updating Supplier info",
        "reason": "%REASON%"
    }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.
`reason`	Строка	Причина ошибки.

Пример ошибочного ответа

Ниже приведен пример ответа с ошибкой на запрос *PUT suppliers/{supplier}*.

```
HTTP/1.1 404 Supplier doesn't exist
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 93

[{"status": "An error occurred while updating supplier info", "reason": "Supplier doesn't exist"}]
```

PUT suppliers/{supplier} (режим мультитенантности)

Обновление указанной информации об источнике данных об угрозах в рамках указанного тенанта.

С помощью этого запроса могут обновляться только источники данных об угрозах, созданные с помощью REST API.

Путь

```
/api/%API_VERSION%/{TenantName}/suppliers/{supplier}
```

Метод

`PUT`

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.
`Content-Type`	`application/json`	Тип содержимого запроса. Также можно указать кодировку `utf-8`. Например: `Content-Type: application/json; charset=utf-8`
`Content-Length`	Integer	Размер тела запроса в байтах. Максимальный размер тела этого запроса составляет 128 МБ (`134217728`).

Параметры запроса

Этот запрос имеет следующие параметры:

Параметры запроса

Имя	Тип параметра	Описание
`supplier`	Путь	Имя источника данных об угрозах.

Тело запроса

Тело этого запроса содержит массив JSON с объектом источника данных об угрозах. Должен быть указан только один объект источника данных об угрозах.

```
[
    {
      "status":"%SUPPLIER_STATUS%"
    }
]
```

Свойства объекта источника данных об угрозах описаны в следующей таблице.

Свойства объекта источника данных об угрозах

Свойство	Значение	Обязательное	Описание
`status`	Строка	Нет	Статус источника данных об угрозах. Если источник данных об угрозах требуется включить, значение должно быть `enabled`. Если источник данных об угрозах требуется отключить, значение должно быть `disabled`.

Пример запроса

Ниже приведен пример запроса *PUT suppliers/{supplier}*.

```
PUT https://192.168.2.57/api/1.3/ExampleTenant/suppliers/ExampleSupplier

Accept: application/json
Content-Type: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
Content-Length: 41

[
 {"status":"enabled"}
]
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит объект JSON со статусом операции.

```
[
    {
        "status": "Supplier info successfully updated"
    }
]
```

Свойства объекта статуса описаны в следующей таблице.

Свойства объекта статуса

Свойство	Значение	Описание
`status`	Строка	Статус операции.

Пример ответа

Ниже приведен пример ответа на запрос *PUT suppliers/{supplier}*.

```
HTTP/1.3 201 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 46

[{"status": "Supplier info successfully updated"}]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
    {
        "status": "An error occurred while updating Supplier info",
        "reason": "%REASON%"
    }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.
`reason`	Строка	Причина ошибки.

Пример ошибочного ответа

Ниже приведен пример ответа с ошибкой на запрос *PUT suppliers/{supplier}*.

```
HTTP/1.3 404 Supplier doesn't exist
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 93

[{"status": "An error occurred while updating supplier info", "reason": "Supplier doesn't exist"}]
```

DELETE suppliers/{supplier}

Удаление указанного поставщика.

С помощью этого запроса могут удаляться только источники данных об угрозах, созданные с помощью REST API.

Путь

```
/api/%API_VERSION%/suppliers/{supplier}
```

Метод

```
DELETE
```

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.

Параметры запроса

Этот запрос имеет следующие параметры:

Параметры запроса

Имя	Тип параметра	Описание
`supplier`	Путь	Имя источника данных об угрозах.

Тело запроса

Тело этого запроса пустое.

Пример запроса

Ниже приведен пример запроса *DELETE suppliers/{supplier}*.

```
DELETE https://192.168.2.57/api/1.1/suppliers/ExampleSupplier

Accept: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит объект JSON со статусом операции.

```
[
    {
        "status": "Supplier successfully removed"
    }
]
```

Свойства объекта статуса описаны в следующей таблице.

Свойства объекта статуса

Свойство	Значение	Описание
`status`	Строка	Статус операции.

Пример ответа

Ниже приведен пример ответа на запрос *DELETE suppliers/{supplier}*.

```
HTTP/1.1 201 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 46

[{"status": "Supplier successfully removed"}]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
    {
        "status": "An error occurred while removing the supplier",
        "reason": "%REASON%"
    }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.
`reason`	Строка	Причина ошибки. Это свойство может отсутствовать в ответе.

Пример ошибочного ответа

Ниже приведен пример ответа с ошибкой на запрос *DELETE suppliers/{supplier}*.

```
HTTP/1.1 404 Supplier doesn't exist
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 86

[{"status": "An error occurred while removing the supplier", "reason": "Supplier doesn't exist"}]
```

PUT suppliers/{supplier}/indicators

Добавление новых индикаторов в источник данных об угрозах и обновление существующих индикаторов.

С помощью этого запроса можно обновить только источники данных, созданные с помощью REST API, а также источники данных *InternalTI* и *FalsePositive*.

Путь

```
/api/%API_VERSION%/suppliers/{supplier}/indicators
```

Метод

`PUT`

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.
`Content-Type`	`application/json`	Тип содержимого запроса. Также можно указать кодировку `utf-8`. Например: `Content-Type: application/json; charset=utf-8`
`Content-Length`	Integer	Размер тела запроса в байтах. Максимальный размер тела этого запроса составляет 128 МБ (`134217728`).

Параметры запроса

Этот запрос имеет следующие параметры:

Параметры запроса

Имя	Тип параметра	Описание
`supplier`	Путь	Имя источника данных об угрозах.

Тело запроса

Тело этого запроса содержит массив объектов индикаторов в формате JSON.

```
[
    {
      "indicator":"%INDICATOR_VALUE_1%",
      "context":
         {
           "%FIELD_NAME_1%":"%FIELD_VALUE_1%",
            ...
           "%FIELD_NAME_N%":"%FIELD_VALUE_N%"
         },
      "tags":
         [
           "%TAG_NAME_1%",
            ...
           "%TAG_NAME_N%"
       ]
    },
    ...
    {
      "indicator":"%INDICATOR_VALUE_N%",
      "context":
         {
```

```
            "%FIELD_NAME_1%":"%FIELD_VALUE_1%",
             ...
            "%FIELD_NAME_N%":"%FIELD_VALUE_N%"
          }
    }
]
```

Свойства объекта индикатора описаны в следующей таблице.

Свойства объекта индикатора

Свойство	Значение	Обязательное	Описание
`indicator`	Строка	Да	Значение индикатора. Можно указать следующие типы индикаторов: • Хеш MD5 • SHA1 Hash • Хеш SHA256 • IP Address • URL
`context`	Объект контекста индикатора	Нет (см. описание)	Контекст индикатора. Это свойство должно содержать объект контекста индикатора. Если индикаторы добавляются к источнику данных об угрозах *FalsePositive*, свойство *context* не указывается.
`tags`	Объект тегов индикатора	Нет	Доступно, начиная с REST API 1.1. Список тегов, назначенных индикатору. Список должен содержать только те теги, которые уже есть в базе данных Kaspersky CyberTrace. Для добавления нового тега в базу данных следует использовать запрос POST tags. Если объект тегов индикаторов отсутствует, Kaspersky CyberTrace не изменяет информацию о тегах индикаторов в базе данных. Если передан пустой объект тегов индикаторов, Kaspersky CyberTrace снимает все теги с индикатора в базе данных. Сами теги при этом не удаляются. При добавлении или изменении имен тегов Kaspersky CyberTrace преобразует буквы в верхний регистр.
`mark_detections`	Boolean	Нет	Доступно, начиная с REST API 1.2. Флажок, указывающий на то, что связанные с индикатором обнаруженные киберугрозы являются ложными срабатываниями. Этот параметр используется только в том случае, если в пути запроса для источника данных об угрозах было указано значение `FalsePositive`.

Свойства объекта контекста индикатора описаны в следующей таблице.

Свойства объекта контекста индикатора

Свойство	Значение	Обязательное	Описание
`%FIELD_NAME%`	`%FIELD_VALUE%`	Да	Одно или несколько полей контекста для индикатора. Название свойства должно соответствовать названию поля контекста индикатора. Значение свойства должно соответствовать значению поля контекста индикатора.

Пример запроса

Ниже приведен пример запроса *PUT suppliers/{supplier}/indicators*.

```
PUT https://192.168.2.57/api/1.1/ suppliers /ExampleSupplier/indicators

Accept: application/json
Content-Type: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
Content-Length: 150

[
    {"indicator":"tux.example.com","context":{"ip":"192.0.2.42","name":"ExampleIndicator",
"threat_level":1},"tags":["OSINT", "EXAMPLE"]},
    {"indicator":"malicious.example.com"}
]
```

Ниже приведен пример запроса *PUT suppliers/{supplier}/indicators* в случае, когда параметр `mark_detections` был применен к источнику данных об угрозах `FalsePositive`.

```
PUT https://192.168.2.57/api/1.2/suppliers/FalsePositive/indicators
Accept: application/json
Content-Type: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
Content-Length: 150

[
    {
      "indicator":"DC212B238A5A7C0A9DF7BF298546A154",
      "tags":
         [
           "FP"
        ],
       "mark_detections": false
    },
    ...
]
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит объект JSON со статусом операции.

```
[
    {
        "status": "All indicators were successfully added to the database"
```

```
    }
]
```

Свойства объекта статуса описаны в следующей таблице.

Свойства объекта статуса

Свойство	Значение	Описание
`status`	Строка	Статус операции.

Пример ответа

Ниже приведен пример ответа на запрос *PUT suppliers/{supplier}/indicators*.

```
HTTP/1.1 201 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 46

[{"status": "All indicators successfully added to the database"}]
```

Ответ о частичном успехе

Этот ответ генерируется, если успешно обработаны были не все индикаторы.

Тело ответа содержит объект частичного успеха со статусом операции и массив объектов ошибок индикатора:

```
[
    {
        "status": "An error occurred while adding some of the indicators to the
database",
        "error_indicators":[
            {
                "indicator": "%INDICATOR_VALUE_1%",
                "reason": "%REASON%"
            },
                ...
            {
                "indicator": "%INDICATOR_VALUE_N%",
                "reason": "%REASON%"
            }
        ]
    }
]
```

Свойства объекта частичного успеха описаны в следующей таблице.

Свойства объекта частичного успеха

Свойство	Значение	Описание
`status`	Строка	Статус операции.
`error_indicators`	Объекты ошибок индикатора	Массив информации об индикаторах, которые не были обработаны.

Свойства объекта ошибки индикатора описаны в следующей таблице.

Свойства объекта ошибки индикатора

Свойство	Значение	Описание
`indicator`	Строка	Индикатор, который не был обработан.
`reason`	Строка	Причина ошибки. Это свойство может отсутствовать в ответе.

Пример ответа о частичном успехе

Ниже приведен пример ответа о частичном успехе на запрос *PUT suppliers/{supplier}/indicators*.

```
HTTP/1.1 202 Partial success
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 265

[{"status": "An error occurred while adding some of the indicators to the database","error_indicators":
[{"indicator":"bad\.example.com", "reason": "Invalid indicator format"},{"indicator":"bad2.example.com
bad3.example.com", "reason": "Invalid indicator format"}]}]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
    {
        "status": "An error occurred while adding indicators to the database",
    }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.

Пример ошибочного ответа

Ниже приведен пример ответа с ошибкой на запрос *PUT suppliers/{supplier}*.

```
HTTP/1.1 500 Internal Server Error
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 73

[{"status": "An error occurred while adding indicators to the database"}]
```

PUT suppliers/{supplier}/indicators (режим мультитенантности)

Добавление в источник данных об угрозах новых индикаторов и обновление существующих индикаторов в рамках указанного тенанта.

С помощью этого запроса можно обновить только источники данных, созданные с помощью REST API, а также источники данных *InternalTI* и *FalsePositive*.

Путь

`/api/%API_VERSION%/{TenantName}/suppliers/{supplier}/indicators`

Метод

`PUT`

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.
`Content-Type`	`application/json`	Тип содержимого запроса. Также можно указать кодировку `utf-8`. Например: `Content-Type: application/json; charset=utf-8`
`Content-Length`	Integer	Размер тела запроса в байтах. Максимальный размер тела этого запроса составляет 128 МБ (`134217728`).

Параметры запроса

Этот запрос имеет следующие параметры:

Параметры запроса

Имя	Тип параметра	Описание
`supplier`	Путь	Имя источника данных об угрозах.

Тело запроса

Тело этого запроса содержит массив объектов индикаторов в формате JSON.

```
[
    {
      "indicator":"%INDICATOR_VALUE_1%",
      "context":
         {
           "%FIELD_NAME_1%":"%FIELD_VALUE_1%",
            ...
           "%FIELD_NAME_N%":"%FIELD_VALUE_N%"
         },
      "tags":
         [
           "%TAG_NAME_1%",
            ...
           "%TAG_NAME_N%"
        ]
    },
    ...
    {
      "indicator":"%INDICATOR_VALUE_N%",
      "context":
         {
           "%FIELD_NAME_1%":"%FIELD_VALUE_1%",
            ...
           "%FIELD_NAME_N%":"%FIELD_VALUE_N%"
         }
    }
]
```

Свойства объекта индикатора описаны в следующей таблице.

Свойства объекта индикатора

Свойство	Значение	Обязательное	Описание
`indicator`	Строка	Да	Значение индикатора. Можно указать следующие типы индикаторов: • Хеш MD5 • SHA1 Hash • Хеш SHA256 • IP Address • URL

Свойство	Значение	Обязательное	Описание
`context`	Объект контекста индикатора	Нет (см. описание)	Контекст индикатора. Это свойство должно содержать объект контекста индикатора. Если индикаторы добавляются к источнику данных об угрозах *FalsePositive*, свойство *context* не указывается.
`tags`	Объект тегов индикатора	Нет	Доступно, начиная с REST API 1.1. Список тегов, назначенных индикатору. Список должен содержать только те теги, которые уже есть в базе данных Kaspersky CyberTrace. Для добавления нового тега в базу данных следует использовать запрос POST tags. Если объект тегов индикаторов отсутствует, Kaspersky CyberTrace не изменяет информацию о тегах индикаторов в базе данных. Если передан пустой объект тегов индикаторов, Kaspersky CyberTrace снимает все теги с индикатора в базе данных. Сами теги при этом не удаляются. При добавлении или изменении имен тегов Kaspersky CyberTrace преобразует буквы в верхний регистр.
`mark_detections`	Boolean	Нет	Доступно, начиная с REST API 1.2. Флажок, указывающий на то, что связанные с индикатором обнаруженные киберугрозы являются ложными срабатываниями. Этот параметр используется только в том случае, если в пути запроса для источника данных об угрозах было указано значение `FalsePositive`.

Свойства объекта контекста индикатора описаны в следующей таблице.

Свойства объекта контекста индикатора

Свойство	Значение	Обязательное	Описание
`%FIELD_NAME%`	`%FIELD_VALUE%`	Да	Одно или несколько полей контекста для индикатора. Название свойства должно соответствовать названию поля контекста индикатора. Значение свойства должно соответствовать значению поля контекста индикатора.

Пример запроса

Ниже приведен пример запроса *PUT suppliers/{supplier}/indicators*.

```
PUT https://192.168.2.57/api/1.3/ExampleTenant/ suppliers /ExampleSupplier/indicators

Accept: application/json
Content-Type: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
Content-Length: 150

[
    {"indicator":"tux.example.com","context":{"ip":"192.0.2.42","name":"ExampleIndicator",
"threat_level":1},"tags":["OSINT", "EXAMPLE"]},
    {"indicator":"malicious.example.com"}
]
```

Ниже приведен пример запроса *PUT suppliers/{supplier}/indicators* в случае, когда параметр `mark_detections` был применен к источнику данных об угрозах `FalsePositive`.

```
PUT https://192.168.2.57/api/1.3/ExampleTenant/suppliers/FalsePositive/indicators
Accept: application/json
Content-Type: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
Content-Length: 150

[
    {
      "indicator":"DC212B238A5A7C0A9DF7BF298546A154",
      "tags":
         [
           "FP"
        ],
       "mark_detections": false
    },
    ...
]
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит объект JSON со статусом операции.

```
[
    {
        "status": "All indicators were successfully added to the database"
    }
]
```

Свойства объекта статуса описаны в следующей таблице.

Свойства объекта статуса

Свойство	Значение	Описание
`status`	Строка	Статус операции.

Пример ответа

Ниже приведен пример ответа на запрос *PUT suppliers/{supplier}/indicators*.

```
HTTP/1.3 201 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 46

[{"status": "All indicators successfully added to the database"}]
```

Ответ о частичном успехе

Этот ответ генерируется, если успешно обработаны были не все индикаторы.

Тело ответа содержит объект частичного успеха со статусом операции и массив объектов ошибок индикатора:

```
[
    {
        "status": "An error occurred while adding some of the indicators to the
database",
        "error_indicators":[
            {
                "indicator": "%INDICATOR_VALUE_1%",
                "reason": "%REASON%"
            },
                ...
            {
                "indicator": "%INDICATOR_VALUE_N%",
                "reason": "%REASON%"
            }
        ]
    }
]
```

Свойства объекта частичного успеха описаны в следующей таблице.

Свойства объекта частичного успеха

Свойство	Значение	Описание
`status`	Строка	Статус операции.
`error_indicators`	Объекты ошибок индикатора	Массив информации об индикаторах, которые не были обработаны.

Свойства объекта ошибки индикатора описаны в следующей таблице.

Свойства объекта ошибки индикатора

Свойство	Значение	Описание
`indicator`	Строка	Индикатор, который не был обработан.
`reason`	Строка	Причина ошибки. Это свойство может отсутствовать в ответе.

Пример ответа о частичном успехе

Ниже приведен пример ответа о частичном успехе на запрос *PUT suppliers/{supplier}/indicators*.

```
HTTP/1.3 202 Partial success
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 265

[{"status": "An error occurred while adding some of the indicators to the database","error_indicators":
[{"indicator":"bad\.example.com", "reason": "Invalid indicator format"},{"indicator":"bad2.example.com
bad3.example.com", "reason": "Invalid indicator format"}]}]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
    {
        "status": "An error occurred while adding indicators to the database",
    }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.

Пример ошибочного ответа

Ниже приведен пример ответа с ошибкой на запрос *PUT suppliers/{supplier}*.

```
HTTP/1.3 500 Internal Server Error
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 73

[{"status": "An error occurred while adding indicators to the database"}]
```

DELETE suppliers/{supplier}/indicators

Удаляет указанные индикаторы из источников данных, включая источники *InternalTI* и *FalsePositive*.

С помощью этого запроса можно удалить индикаторы только из источников данных, созданных с помощью REST API, а также из источников *InternalTI* и *FalsePositive*.

Путь

```
/api/%API_VERSION%/suppliers/{supplier}/indicators
```

Метод

```
DELETE
```

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.
`Content-Type`	`application/json`	Тип содержимого запроса. Также можно указать кодировку `utf-8`. Например: `Content-Type: application/json; charset=utf-8`
`Content-Length`	`Integer`	Размер тела запроса в байтах. Максимальный размер тела этого запроса составляет 64 МБ (`67108864`).

Параметры запроса

Этот запрос имеет следующие параметры:

Параметры запроса

Имя	Тип параметра	Описание
`supplier`	Путь	Имя источника данных об угрозах.

Тело запроса

Тело этого запроса содержит массив объектов индикаторов в формате JSON.

```
[
    {
      "indicator":"%INDICATOR_VALUE_1%",
    },
    ...
    {
      "indicator":"%INDICATOR_VALUE_N%",
```

```
    }
]
```

Свойства объекта индикатора описаны в следующей таблице.

Свойства объекта индикатора

Свойство	Значение	Обязательное	Описание
`indicator`	Строка	Да	Индикатор, который необходимо удалить. Можно указать следующие типы индикаторов: • Хеш MD5 • SHA1 Hash • Хеш SHA256 • IP Address • URL
`unmark_detections`	Логический оператор	Нет	Доступно, начиная с REST API 1.2. Флажок, указывающий на то, что связанные с индикатором обнаруженные киберугрозы не являются ложными срабатываниями. Этот параметр используется только в том случае, если в пути запроса для источника данных об угрозах было указано значение `FalsePositive`.

Пример запроса

Ниже приведен пример запроса *DELETE suppliers/{supplier}/indicators*.

```
DELETE https://192.168.2.57/api/1.1/suppliers/ExampleSupplier/indicators

Accept: application/json
Content-Type: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
Content-Length: 77

[
    {"indicator":"tux.example.com"},
    {"indicator":"malicious.example.com"}
]
```

Ниже приведен пример запроса *DELETE suppliers/{supplier}/indicators* в случае, когда параметр `unmark_detections` был применен к источнику данных об угрозах `FalsePositive`.

```
DELETE https://192.168.2.57/api/1.2/suppliers/FalsePositive/indicators
Accept: application/json
Content-Type: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
Content-Length: 110

[
    {
      "indicator":"DC212B238A5A7C0A9DF7BF298546A154",
      "unmark_detections": false
    },
    ...
]
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит объект JSON со статусом операции.

```
[
    {
        "status": "All indicators were successfully deleted from the database"
    }
]
```

Свойства объекта статуса описаны в следующей таблице.

Свойства объекта статуса

Свойство	Значение	Описание
`status`	Строка	Статус операции.

Пример ответа

Ниже приведен пример ответа на запрос *DELETE suppliers/{supplier}/indicators*.

```
HTTP/1.1 201 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 74

[{"status": "All indicators were successfully deleted from the database"}]
```

Ответ о частичном успехе

Этот ответ генерируется, если успешно удалены были не все индикаторы.

Тело ответа содержит объект частичного успеха со статусом операции и массив объектов ошибок индикатора:

```
[
```

```
    {
        "status": "An error occurred while deleting some of the indicators from the
database",
        "error_indicators":[
            {
                "indicator": "%INDICATOR_VALUE_1%",
                "reason": "%REASON%"
            },
                ...
            {
                "indicator": "%INDICATOR_VALUE_N%",
                "reason": "%REASON%"
            }
        ]
    }
]
```

Свойства объекта частичного успеха описаны в следующей таблице.

Свойства объекта частичного успеха

Свойство	Значение	Описание
`status`	Строка	Статус операции.
`error_indicators`	Объекты ошибок индикатора	Массив информации об индикаторах, которые не были удалены.

Свойства объекта ошибки индикатора описаны в следующей таблице.

Свойства объекта ошибки индикатора

Свойство	Значение	Описание
`indicator`	Строка	Индикатор, который не был удален.
`reason`	Строка	Причина ошибки. Это свойство может отсутствовать в ответе.

Пример ответа о частичном успехе

Ниже приведен пример ответа о частичном успехе на запрос *DELETE suppliers/{supplier}/indicators*.

```
HTTP/1.1 202 Partial success
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 251

[{"status": "An error occurred while deleting some of the indicators from the database","error_indicators":
[{"indicator":"bad.example.com", "reason": "Indicator doesn't exist"},{"indicator":"bad2\.example.com", "reason":
"Invalid indicator format"}]}]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
    {
        "status": "An error occurred while deleting indicators from the database",
    }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.

Пример ошибочного ответа

Ниже приведен пример ответа с ошибкой на запрос *PUT suppliers/{supplier}*.

```
HTTP/1.1 500 Internal Server Error
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 77

[{"status": "An error occurred while deleting indicators from the database"}]
```

DELETE suppliers/{supplier}/indicators (режим мультитенантности)

Удаляет указанные индикаторы из источника данных об угрозах, включая источники *InternalTI* и *FalsePositive*, в рамках указанного тенанта.

С помощью этого запроса можно удалить индикаторы только из источников данных, созданных с помощью REST API, а также из источников *InternalTI* и *FalsePositive*.

Путь

```
/api/%API_VERSION%/{TenantName}/suppliers/{supplier}/indicators
```

Метод

```
DELETE
```

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.
`Content-Type`	`application/json`	Тип содержимого запроса. Также можно указать кодировку `utf-8`. Например: `Content-Type: application/json; charset=utf-8`
`Content-Length`	Integer	Размер тела запроса в байтах. Максимальный размер тела этого запроса составляет 64 МБ (`67108864`).

Параметры запроса

Этот запрос имеет следующие параметры:

Параметры запроса

Имя	Тип параметра	Описание
`supplier`	Путь	Имя источника данных об угрозах.

Тело запроса

Тело этого запроса содержит массив объектов индикаторов в формате JSON.

```
[
    {
      "indicator":"%INDICATOR_VALUE_1%",
    },
    ...
    {
      "indicator":"%INDICATOR_VALUE_N%",
    }
]
```

Свойства объекта индикатора описаны в следующей таблице.

Свойства объекта индикатора

Свойство	Значение	Обязательное	Описание
`indicator`	Строка	Да	Индикатор, который необходимо удалить. Можно указать следующие типы индикаторов: • Хеш MD5 • SHA1 Hash • Хеш SHA256 • IP Address • URL
`unmark_detections`	Логический оператор	Нет	Доступно, начиная с REST API 1.2. Флажок, указывающий на то, что связанные с индикатором обнаруженные киберугрозы не являются ложными срабатываниями. Этот параметр используется только в том случае, если в пути запроса для источника данных об угрозах было указано значение `FalsePositive`.

Пример запроса

Ниже приведен пример запроса *DELETE suppliers/{supplier}/indicators*.

```
DELETE https://192.168.2.57/api/1.3/ExampleTenant/ suppliers /ExampleSupplier/indicators

Accept: application/json
Content-Type: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
Content-Length: 77

[
    {"indicator":"tux.example.com"},
    {"indicator":"malicious.example.com"}
]
```

Ниже приведен пример запроса *DELETE suppliers/{supplier}/indicators* в случае, когда параметр `unmark_detections` был применен к источнику данных об угрозах `FalsePositive`.

```
DELETE https://192.168.2.57/api/1.3/ExampleTenant/suppliers/FalsePositive/indicators
Accept: application/json
Content-Type: application/json
Authorization: Basic dXNlcjpwYXNzd29yZA==
Content-Length: 110

[
    {
      "indicator":"DC212B238A5A7C0A9DF7BF298546A154",
      "unmark_detections": false
    },
    ...
]
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит объект JSON со статусом операции.

```
[
    {
        "status": "All indicators were successfully deleted from the database"
    }
]
```

Свойства объекта статуса описаны в следующей таблице.

Свойства объекта статуса

Свойство	Значение	Описание
`status`	Строка	Статус операции.

Пример ответа

Ниже приведен пример ответа на запрос *DELETE suppliers/{supplier}/indicators*.

```
HTTP/1.3 201 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 74

[{"status": "All indicators were successfully deleted from the database"}]
```

Ответ о частичном успехе

Этот ответ генерируется, если успешно удалены были не все индикаторы.

Тело ответа содержит объект частичного успеха со статусом операции и массив объектов ошибок индикатора:

```
[
    {
        "status": "An error occurred while deleting some of the indicators from the
database",
        "error_indicators":[
            {
                "indicator": "%INDICATOR_VALUE_1%",
                "reason": "%REASON%"
```

```
            },
                ...
            {
                "indicator": "%INDICATOR_VALUE_N%",
                "reason": "%REASON%"
            }
        ]
    }
]
```

Свойства объекта частичного успеха описаны в следующей таблице.

Свойства объекта частичного успеха

Свойство	Значение	Описание
`status`	Строка	Статус операции.
`error_indicators`	Объекты ошибок индикатора	Массив информации об индикаторах, которые не были удалены.

Свойства объекта ошибки индикатора описаны в следующей таблице.

Свойства объекта ошибки индикатора

Свойство	Значение	Описание
`indicator`	Строка	Индикатор, который не был удален.
`reason`	Строка	Причина ошибки. Это свойство может отсутствовать в ответе.

Пример ответа о частичном успехе

Ниже приведен пример ответа о частичном успехе на запрос *DELETE suppliers/{supplier}/indicators*.

```
HTTP/1.3 202 Partial success
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 251

[{"status": "An error occurred while deleting some of the indicators from the database","error_indicators":
[{"indicator":"bad.example.com", "reason": "Indicator doesn't exist"},{"indicator":"bad2\.example.com", "reason":
"Invalid indicator format"}]}]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
    {
        "status": "An error occurred while deleting indicators from the database",
    }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.

Пример ошибочного ответа

Ниже приведен пример ответа с ошибкой на запрос *PUT suppliers/{supplier}*.

```
HTTP/1.3 500 Internal Server Error
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 77

[{"status": "An error occurred while deleting indicators from the database"}]
```

GET tags

Получение списка тегов.

Путь

`/api/%API_VERSION%/tags`

Метод

`GET`

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.

Тело запроса

Тело этого запроса пустое.

Пример запроса

Ниже приведен пример запроса *GET tags*.

```
GET https://192.168.2.57/api/1.1/tags

Accept: application/json
Authorization: Basic AWxhZGRpbjpvcGVuc2VzYW23
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит массив JSON, содержащий объекты тегов.

```
[
  {
    "name": "%TAG_NAME_1%",
    "weight": %TAG_WEIGHT_1%
  },
  ...
  {
    "name": "%TAG_NAME_N%",
    "weight": %TAG_WEIGHT_N%
  }
]
```

Свойства объекта тега описаны в следующей таблице.

Свойства объекта тега

Свойство	Значение	Описание
`name`	Строка	Имя тега.
`weight`	Целое число	Важность тега от `0` (наименьшая важность) до `5` (наибольшая важность).

Пример ответа

Ниже приведен пример ответа на запрос *GET tags*.

```
HTTP/1.1 200 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 150

[
  {
    "name": "WIN-TROJAN",
    "weight": 5
  },
  {
    "name": "KASPERSKY",
    "weight": 5
  },
  {
    "name": "OSINT",
    "weight": 2
  }
]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
  {
    "status": "An error occurred while getting tags list";
    "reason": "%REASON%"
  }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.
`reason`	Строка	Причина ошибки. Это свойство может отсутствовать.

POST tags

Добавление нового тега.

Путь

`/api/%API_VERSION%/tags`

Метод

`POST`

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.
`Content-Type`	`application/json`	Тип содержимого запроса. Также можно указать кодировку `utf-8`. Например: `Content-Type: application/json; charset=utf-8`
`Content-Length`	Integer	Размер тела запроса в байтах. Максимальный размер тела этого запроса составляет 128 МБ (`134217728`).

Тело запроса

Тело этого запроса содержит массив JSON с объектом тега. Должен быть указан только один объект тега.

```
[
  {
    "name":"%TAG_NAME%",
    "weight": TAG_WEIGHT
  }
]
```

Свойства объекта тега описаны в следующей таблице.

Свойства объекта тега

Свойство	Значение	Обязательное	Описание
`name`	Строка	Да	Имя тега. Длина тега должна составлять от 1 до 128 символов. Тег может содержать латинские буквы, цифры, дефисы (-) и знаки подчеркивания (_). Для нового тега нельзя использовать имя уже существующего тега. При добавлении имен тегов Kaspersky CyberTrace преобразует буквы в верхний регистр.
`weight`	Целое число	Да	Важность тега. Диапазон значений этого параметра: от `0` (наименьшая важность) до `5` (наибольшая важность).

Пример запроса

Ниже приведен пример запроса *POST tags*.

```
POST https://192.168.2.57/api/1.1/tags

Accept: application/json
Content-Type: application/json
Authorization: Basic AWxhZGRpbjpvcGVuc2VzYW23
Content-Length: 150

[
  {
    "name": "WIN-TROJAN",
    "weight": 5
  }
]
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит объект JSON со статусом операции.

```
[
    {
        "status": "Tag successfully created"
    }
]
```

Свойства объекта статуса описаны в следующей таблице.

Свойства объекта статуса

Свойство	Значение	Описание
`status`	Строка	Статус операции.

Пример ответа

Ниже приведен пример ответа на запрос *POST suppliers*.

```
HTTP/1.1 201 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 150

[
  {
    "status": "Tag successfully created"
  }
]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
    {
        "status": "An error occurred while creating tag",
        "reason": "%REASON%"
    }
]
```

GET tags/{tag}

Получение информации об указанном теге.

Путь

```
/api/%API_VERSION%/tags/{tag}
```

Метод

```
GET
```

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.

Параметры запроса

Этот запрос имеет следующие параметры:

Параметры запроса

Имя	Тип параметра	Описание
`tag`	Путь	Имя тега.

Тело запроса

Тело этого запроса пустое.

Пример запроса

Ниже приведен пример запроса *GET tags/{tag}*.

```
GET https://192.168.2.57/api/1.1/tags/WIN-TROJAN

Accept: application/json
Authorization: Basic AWxhZGRpbjpvcGVuc2VzYW23
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит массив JSON с объектом тега.

```
[
  {
    "name": "%TAG_NAME%",
    "weight": %TAG_WEIGHT%
  }
]
```

Свойства объекта тега описаны в следующей таблице.

Свойства объекта тега

Свойство	Значение	Описание
`name`	Строка	Имя тега.
`weight`	Целое число	Важность тега от `0` (наименьшая важность) до `5` (наибольшая важность).

Пример ответа

Ниже приведен пример ответа на запрос *GET tags/{tag}*.

```
HTTP/1.1 200 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 150

[
  {
    "name": "WIN-TROJAN",
    "weight": 5
  }
]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
  {
    "status": "An error occurred while getting tag info",
    "reason": "Tag doesn't exist"
  }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.
`reason`	Строка	Причина ошибки. Это свойство может отсутствовать.

Пример ошибочного ответа

Ниже приведен пример ответа с ошибкой на запрос *GET tags/{tag}*.

```
HTTP/1.1 404 Tag doesn't exist
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 150

[
  {
    "status": "An error occurred while getting tag info",
    "reason": "Tag doesn't exist"
  }
]
```

PUT tags/{tag}

Обновление указанного тега.

Путь

`api/%API_VERSION%/tags/{tag}`

Метод

`PUT`

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.
`Content-Type`	`application/json`	Тип содержимого запроса. Также можно указать кодировку `utf-8`. Например: `Content-Type: application/json; charset=utf-8`
`Content-Length`	Integer	Размер тела запроса в байтах. Максимальный размер тела этого запроса составляет 128 МБ (`134217728`).

Параметры запроса

Этот запрос имеет следующие параметры:

Параметры запроса

Имя	Тип параметра	Описание
`tag`	Путь	Имя тега.

Тело запроса

Тело этого запроса содержит массив JSON с объектом тега. Должен быть указан только один объект тега.

```
[
  {
    "name":"%TAG_NAME%",
    "weight": TAG_WEIGHT
  }
]
```

Свойства объекта тега описаны в следующей таблице.

Свойства объекта тега

Свойство	Значение	Обязательное	Описание
`name`	Строка	Нет	Имя тега. Длина тега должна составлять от 1 до 128 символов. Тег может содержать латинские буквы, цифры, дефисы (-) и знаки подчеркивания (_). Для нового тега нельзя использовать имя уже существующего тега. При изменении имен тегов Kaspersky CyberTrace преобразует буквы в верхний регистр.
`weight`	Целое число	Нет	Важность тега от `0` (наименьшая важность) до `5` (наибольшая важность).

Пример запроса

Ниже приведен пример запроса *PUT tags/{tag}*.

```
PUT https://192.168.2.57/api/1.1/tags/WIN-TROJAN

Accept: application/json
Content-Type: application/json
Authorization: Basic AWxhZGRpbjpvcGVuc2VzYW23
Content-Length: 150

[
  {
    "name": "TROJAN",
    "weight": 4
  }
]
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит объект JSON со статусом операции.

```
[
    {
        "status": "Tag successfully updated"
    }
]
```

Свойства объекта статуса описаны в следующей таблице.

Свойства объекта статуса

Свойство	Значение	Описание
`status`	Строка	Статус операции.

Пример ответа

Ниже приведен пример ответа на запрос *PUT tags/{tag}*.

```
HTTP/1.1 200 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 150

[
  {
    "status": "Tag successfully updated"
  }
]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
    {
        "status": "An error occurred while updating tag",
        "reason": "%REASON%"
    }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.
`reason`	Строка	Причина ошибки. Это свойство может отсутствовать.

Пример ошибочного ответа

Ниже приведен пример ответа с ошибкой на запрос *PUT tags/{tag}*.

```
HTTP/1.1 404 Tag doesn't exist
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 150

[
  {
    "status": "An error occurred while updating tag",
    "reason": "Tag doesn't exist"
  }
]
```

DELETE tags/{tag}

Удаление указанного тега.

Путь

`/api/%API_VERSION%/tags/{tag}`

Метод

`DELETE`

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.

Параметры запроса

Этот запрос имеет следующие параметры:

Параметры запроса

Имя	Тип параметра	Описание
`tag`	Путь	Имя тега.

Тело запроса

Тело этого запроса пустое.

Пример запроса

Ниже приведен пример запроса *DELETE tags/{tag}*.

```
DELETE https://192.168.2.57/api/1.1/tags/WIN-TROJAN

Accept: application/json
Authorization: Basic AWxhZGRpbjpvcGVuc2VzYW23
```

Заголовки ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа

Тело ответа содержит объект JSON со статусом операции.

```
[
    {
        "status": "Tag successfully deleted"
    }
]
```

Свойства объекта статуса описаны в следующей таблице.

Свойства объекта статуса

Свойство	Значение	Описание
`status`	Строка	Статус операции.

Пример ответа

Ниже приведен пример ответа на запрос *DELETE tags/{tag}*.

```
HTTP/1.1 200 OK
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 150

[
  {
    "status": "Tag successfully deleted"
  }
]
```

Ответы с ошибкой

Ответы с ошибкой содержат информацию о статусе ответа.

Ответ с ошибкой содержит объект JSON с описанием ошибки.

```
[
    {
        "status": "An error occurred while removing tag",
        "reason": "%REASON%"
    }
]
```

Описание свойств объекта ошибки приведено в следующей таблице.

Свойства объекта ошибки

Свойство	Значение	Описание
`status`	Строка	Описание ошибки.
`reason`	Строка	Причина ошибки. Это свойство может отсутствовать.

Пример ошибочного ответа

Ниже приведен пример ответа с ошибкой на запрос *DELETE suppliers/{supplier}*.

```
HTTP/1.1 404 Tag doesn't exist
Date:Mon, 23 Dec 2019 09:56:10 UTC
Content-Type: application/json
Content-Length: 150

[
  {
    "status": "An error occurred while removing tag",
    "reason": "Tag doesn't exists"
  }
]
```

PUT publicAPI

Позволяет сохранять обнаружения индикаторов, полученных через общедоступные API. Эта функция доступна для всех тенантов.

Путь

`/api/%API_VERSION%/{TenantName}/settings/publicApi`

Метод

`PUT`

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого запроса. Также можно указать кодировку `utf-8`. Например: `Content-Type: application/json; charset=utf-8`
`Content-Length`	Integer	Размер тела запроса в байтах. Максимальный размер тела этого запроса составляет 128 МБ (`134217728`).

Тело запроса

Тело запроса имеет следующий формат:

```
{
    "saveDetects":%STATUS%
}
```

Описание свойств объекта статуса функции приведено в следующей таблице.

Свойства объекта статуса функции

Свойство	Значение	Обязательное	Описание
saveDetects	Логический оператор	Да	Включение или выключение функции.

Пример запроса

```
PUT https://192.168.2.57/api/1.3/ExampleTenant/settings/publicApi

Content-Type: application/json
Content-Length: 150

[
  {
    "saveDetects": true
  }
]
```

Тело ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
Content-Type	application/json	Тип содержимого ответа.
Content-Length	Integer	Размер тела ответа в байтах.

Тело ответа имеет следующий формат:

```
{
        "status":"%TEXT%"
}
```

Свойства объекта статуса описаны в следующей таблице.

Свойства объекта статуса

Свойство	Значение	Описание
`status`	Строка	Статус операции.

Пример ответа

```
HTTP/1.3 200 OK
Date:Mon, 21 Apr 2025 09:56:10 UTC
Content-Type: application/json
Content-Length: 67

[
  {
    "status": "Settings updated successfully."
  }
]
```

GET publicAPI

Получает от тенанта статус функции сохранения обнаружений индикаторов, полученных через общедоступные API.

Путь

`/api/%API_VERSION%/{TenantName}/settings/publicApi`

Метод

`GET`

Заголовки запроса

Этот запрос имеет следующие заголовки:

Заголовки запроса

Имя	Значение	Описание
`Authorization`	String (base 64)	Строка аутентификации.
`Accept`	`application/json`	Тип содержимого ответа.

Тело запроса

Тело этого запроса пустое.

Пример запроса

```
GET https://192.168.2.57/api/1.3/ExampleTenant/settings/publicApi

Accept: application/json
Authorization: Basic AWxhZGRpbjpvcGVuc2VzYW23
```

Тело ответа

Ответ имеет следующие заголовки.

Заголовки ответа

Имя	Значение	Описание
`Content-Type`	`application/json`	Тип содержимого ответа.
`Content-Length`	Integer	Размер тела ответа в байтах.

Тело ответа имеет следующий формат:

```
{
        "saveDetects": %STATUS%
}
```

Описание свойств объекта статуса функции приведено в следующей таблице.

Свойства объекта статуса функции

Свойство	Значение	Описание
saveDetects	Логический оператор	Статус функции.

Пример ответа

```
HTTP/1.3 200 OK
Date:Mon, 21 Apr 2025 09:56:10 UTC
Content-Type: application/json
Content-Length: 36

[
  {
    "saveDetects": true
  }
]
```

Устранение неполадок

В этом разделе приведена информация, с помощью которой можно решить возможные проблемы при использовании Kaspersky CyberTrace.

Устранение общих неполадок

В этом разделе приведена информация, с помощью которой можно решить возможные проблемы при использовании Kaspersky CyberTrace.

Если при использовании Kaspersky CyberTrace возникли проблемы, проверьте, выполняются ли следующие условия:

- Служба Kaspersky CyberTrace запущена.

  Windows: проверьте статус службы из командной строки с помощью команды `sc query cybertrace`.

  Linux: проверьте статус службы из терминала с помощью команды `systemctl status cybertrace.service`.

- На сервере Kaspersky CyberTrace достаточно свободного места на диске и оперативной памяти.

- Веб-страница https://wlinfo.kaspersky.com доступна с сервера Kaspersky CyberTrace.

  Для проверки этой веб-страницы как в Windows, так и в Linux используется следующая команда: `curl -v --cert /opt/kaspersky/ktfs/dmz/feeds.pem [--proxy user:password@proxy-server.com:3128] https://wlinfo.kaspersky.com/api/v1.0/feeds`

  В результате этой проверки может быть получен список доступных потоков данных об угрозах в соответствии со сертификатом, например:

  ```
  {
    "name": "TI Demo Botnet C&C URL Data Feed",
    "updates":
        {"href": "https://wlinfo.kaspersky.com/api/v1.0/feeds/85/updates"},
    "license":
        {"expires": "2024-02-19T00:00:00"}
  }
  ```

  Если результат содержит ошибку, отправьте вывод этой команды в Службу технической поддержки.

- Источник событий (SIEM) доступен с сервера Kaspersky CyberTrace.

  - Веб-интерфейс:

    Выберите вкладку **Параметры → Служба**. В разделе **Служебные оповещения**, в поле ввода **IP-адрес** введите IP-адрес SIEM, а в поле ввода **Порт** введите порт SIEM.

  - В конфигурационном файле `kl_feed_service.conf` (это необходимо проверить, только если служба Kaspersky CyberTrace не запускается):

    Windows: `\Kaspersky Lab\Kaspersky CyberTrace\bin\kl_feed_service.conf`

    Linux: `opt/kaspersky/ktfs/etc/kl_feed_service.conf`

    Ниже приведен пример настроек из конфигурационного файла:

```
<OutputSettings>
     <ConnectionString>127.0.0.1:9998</ConnectionString>
</OutputSettings>
```

Проверьте порт, используемый источником для подключения к Kaspersky CyberTrace.

Убедитесь, что во встроенном сетевом экране правильно настроен порт для получения событий из источника в Kaspersky CyberTrace.

Убедитесь, что во встроенном сетевом экране на стороне SIEM правильно настроен порт для получения обнаружений киберугроз из Kaspersky CyberTrace.

Если проблема не решена, обратитесь в Службу технической поддержки и приложите следующие данные:

- Конфигурационный файл Kaspersky CyberTrace для Windows: `\Kaspersky Lab\Kaspersky CyberTrace\bin\kl_feed_service.conf`
- Конфигурационный файл Kaspersky CyberTrace для Linux: `opt/kaspersky/ktfs/etc/kl_feed_service.conf`

  Получить конфигурационный файл можно двумя способами:

  - Если доступен веб-интерфейс, выберите **Параметры** → **Служба** → **Экспортировать конфигурационный файл**.
  - Если службу Kaspersky CyberTrace запустить не удается, скопируйте файлы из каталогов и укажите пути для соответствующих операционных систем.
- Файлы журнала Kaspersky CyberTrace уровня «debug»

  Дополнительные сведения приведены в разделах Настройка журналов и Журнал Kaspersky CyberTrace Service.

  > Важно понимать, что в Службу технической поддержки будут отправлены файлы журнала отладки, содержащие полные входящие события.
- Скриншоты, иллюстрирующие проблему.
- Результаты запуска скрипта `collect.sh`.

  Запуск скрипта `collect.sh` создает отчет, содержащий всю основную диагностическую информацию, полученную с сервера.

  > Перед отправкой отчета в Службу технической поддержки удалите из него всю конфиденциальную информацию.

  Подробные указания по созданию отчета приведены по адресу https://support.kaspersky.ru/15732.

Устранение неполадок Feed Utility

В этом разделе приведена информация, с помощью которой можно решить проблемы, которые могут возникнуть при использовании Feed Utility.

Проблемы с сетью

Если Feed Utility не загружает потоки данных об угрозах или если возникла какая-либо проблема, связанная с сетью:

- Убедитесь, что сертификат, указанный в конфигурационном файле, действителен. Сертификат по умолчанию из комплекта поставки можно использовать только для загрузки демонстрационных потоков данных об угрозах.
- Убедитесь, что сеть настроена правильно.

Если Feed Utility должна обращаться к серверам «Лаборатории Касперского» через прокси-сервер, настройте параметры прокси-сервера с помощью команды `--set-proxy`. В этом случае убедитесь, что имя пользователя и пароль для прокси-сервера действительны и не истекли.

Ошибка SSL при загрузке стороннего потока данных об угрозах

Если при загрузке стороннего потока данных об угрозах возникла ошибка SSL, выполните следующие действия:

- В Linux убедитесь, что корневой сертификат для источника стороннего потока данных об угрозах присутствует в `/etc/ssl/certs` или `/etc/pki/tls/certs/ca-bundle.crt`. Если сертификат отсутствует, импортируйте его туда.
- В ОС Windows:

  1. Вызовите команду Windows `Выполнить`.
  2. В диалоговом окне **Выполнить** введите `certlm.msc`.

     Откроется инструмент «Диспетчер сертификатов» для сервера.
  3. Выберите **Сертификаты (локальный сервер)** → **Доверенные корневые центры сертификации** → **Сертификаты**.
  4. Убедитесь, что в этой папке присутствует корневой сертификат для источника сторонних потоков данных об угрозах. Если сертификат отсутствует, импортируйте его в эту папку.

Проблемы с обработкой потоков данных об угрозах

Если Feed Utility не обрабатывает потоки данных об угрозах должным образом, выполните следующие действия:

- Убедитесь, что параметры конфигурационного файла указаны без опечаток. Feed Utility игнорирует имена параметров с опечатками. Например, если вместо параметра `RequiredFields` указан параметр `ReqFields`, Feed Utility будет игнорировать этот параметр.
- Убедитесь, что правила потоков данных об угрозах и правила фильтрации указаны правильно. Например, правила фильтрации могут быть заданы таким образом, что в итоговый поток данных об угрозах не попадают никакие записи.
- Если загрузка и распаковка потоков данных об угрозах (с помощью команд `-d -u`) выполняется отдельно от их обработки (с помощью команды `-p`), Feed Utility может выводить сообщение об ошибке по нескольким версиям исходного файла потока данных об угрозах. Убедитесь, что вы удалили исходные файлы потоков данных об угрозах в каталоге, в который их распаковывает Feed Utility. Feed Utility не делает этого автоматически.

Прочие проблемы

В случае возникновения других проблем обращайтесь по адресу intelligence@kaspersky.com.

Устранение неполадок веб-интерфейса Kaspersky CyberTrace

В этом разделе приведена информация, с помощью которой можно решить проблемы, которые могут возникнуть при использовании веб-интерфейса Kaspersky CyberTrace.

Проблема: я не помню свой пароль

Чтобы решить эту проблему, попробуйте выполнить следующие действия:

- Если роль вашей учетной записи — «Аналитик» или «Менеджер тенанта», обратитесь к своему администратору, чтобы изменить пароль.
- Если роль вашей учетной записи — «Администратор», вы можете изменить пароль для другого пользователя в разделе **Параметры → Пользователи** веб-интерфейса Kaspersky CyberTrace.
- Если роль вашей учетной записи — «Администратор», вы можете сбросить пароль для своей учетной записи с помощью Password Utility.

Проблема: при открытии веб-интерфейса Kaspersky CyberTrace в браузере отображается белый экран

Возможная причина этой проблемы заключается в использовании неподдерживаемого браузера. Убедитесь, что используется один из поддерживаемых браузеров.

Проблема: при обновлении потоков данных об угрозах вручную отображается сообщение об ошибке «Could not update feeds»

Чтобы решить эту проблему, попробуйте выполнить следующее действие:

- Попытайтесь запустить процесс обновления позже. Источником этой проблемы является другой процесс обновления, который выполняется в то же время.

Проблема: ошибка недоверенного соединения при подключении к веб-интерфейсу Kaspersky CyberTrace

SSL-сертификаты, сгенерированные во время установки Kaspersky CyberTrace, являются самоподписанными, поэтому браузер сообщает о недоверенном соединении.

Чтобы решить эту проблему, попробуйте выполнить следующие действия:

- (Рекомендуется) Используйте другие сертификаты, которые являются доверенными в вашей инфраструктуре.
- Если использование других сертификатов невозможно, можно добавить изначально сгенерированный сертификат в качестве доверенного для браузера или операционной системы.

Проблема: срок действия SSL-сертификата истек

SSL-сертификаты, сгенерированные во время установки Kaspersky CyberTrace, действительны в течение двух лет. Если срок действия сертификатов истекает, необходимо сгенерировать новые сертификаты.

Чтобы решить эту проблему, попробуйте выполнить следующие действия:

- В ОС Linux:
  - Выполните в консоли следующую команду:

    ```
    %service_dir%/configure --change
    ```

  - Укажите те же параметры, которые указывались при предыдущей установке Kaspersky CyberTrace.

- В ОС Windows:
  - Запустите исполняемый файл установщика Kaspersky CyberTrace.
  - Нажмите на кнопку **Change**.
  - Укажите те же параметры, которые указывались при предыдущей установке Kaspersky CyberTrace.

Проблема: произошла ошибка при поиске индикаторов из файла журнала или хешей файлов

Эта ошибка может быть вызвана несколькими возможными причинами:

- На сервере, на котором установлен Kaspersky CyberTrace, нет свободного места.

  Рекомендуется сделать следующее:

  - Перезапустите Kaspersky CyberTrace: могут остаться файлы, связанные с предыдущими поисковыми запросами.
  - Удалите ненужные файлы с сервера, на котором установлен Kaspersky CyberTrace.
- Произошла ошибка при попытке открыть файл, выбранный для поиска. Это может произойти, если файл был удален или если у процесса Kaspersky CyberTrace нет прав на чтение файла.
- Убедитесь, что файл не удален и к нему есть доступ.

Проблема: не удается войти в Kaspersky CyberTrace после обновления

Чтобы решить эту проблему, попробуйте выполнить следующие действия:

- Очистите кеш браузера стандартным способом.

Проблема: информация об обнаруженных хешах не отображается на информационной панели

Возможная причина этой проблемы заключается в том, что параметры даты и времени на сервере конечного пользователя отличаются от параметров на сервере, на котором работает Kaspersky CyberTrace, и эта разница во времени слишком велика. Разница во времени не должна превышать 30 минут.

Чтобы решить эту проблему, измените настройки даты и времени на правильные. Для получения точных значений даты и времени можно использовать NTP-сервер.

Проблема: в окне Изменить источник событий "{{sourceId}}" не отображаются входящие события, а кнопки Запустить анализ событий и Возобновить анализ событий не работают.

Чтобы решить эту проблему, обновите KIS до версии 21.5.7.225 в Windows или KES до версии 11.8 в Windows/macOS.

Проблема: потоки данных не обновляются

В непредвиденных ситуациях может возникнуть ошибка обновления потоков данных, в результате чего может быть не выполнено удаление следующих файлов:

```
/feeds/download/.kl_feed_lock
```

```
/tools/output/.kl_feed_lock
```

Если эти файлы не удалены, возникает ошибка обновления потоков данных.

Для решения проблемы удалите эти файлы вручную. Также при обновлении службы убедитесь, что эти файлы отсутствуют.

В нормальных условиях эти файлы удаляются независимо от статуса обновления потоков данных.

Устранение неполадок Splunk

В этом разделе приведена информация, с помощью которой можно решить проблемы, которые могут возникнуть при использовании Kaspersky CyberTrace со Splunk.

Проблема: Kaspersky CyberTrace App не отображает события из Kaspersky CyberTrace Service или отображает их некорректно

Чтобы решить эту проблему, попробуйте выполнить следующие действия:

- Убедитесь, что сервер Kaspersky CyberTrace Service включен и Kaspersky CyberTrace Service работает.
- Убедитесь, что сервер Kaspersky CyberTrace Service доступен с сервера, на котором установлен Splunk. Для этого можно использовать утилиту `ping`.
- Убедитесь, что в конфигурационном файле Kaspersky CyberTrace Service содержится правильная строка подключения для вывода (строку подключения можно проверить на вкладке **Параметры → Служба** в веб-интерфейсе Kaspersky CyberTrace).
- Убедитесь, что в конфигурационном файле Kaspersky CyberTrace App правильно указаны порты и адреса для входящих событий.

- Убедитесь, что указанные порты открыты. Для этого можно использовать утилиту `netcat`.
- Попытайтесь использовать схему интеграции Splunk и Kaspersky CyberTrace Service по умолчанию (в этой схеме форвардер, индексатор и search head устанавливаются на одном сервере).

Проблема: Kaspersky CyberTrace Service не получает события из Splunk

Чтобы решить эту проблему, попробуйте выполнить следующие действия:

- Убедитесь, что сервер Splunk включен и Splunk запущен.
- Убедитесь, что сервер Kaspersky CyberTrace Service доступен с сервера Splunk. Для этого можно использовать утилиту `ping`.
- Убедитесь, что события пересылаются из Splunk в Kaspersky CyberTrace Service. Проверьте правильность указания адресов и портов в конфигурационных файлах Kaspersky CyberTrace App.
- Убедитесь, что порты, указанные в конфигурационных файлах Kaspersky CyberTrace App, открыты на сервере Kaspersky CyberTrace Service. Для этого можно использовать утилиту `netcat`.
- Попробуйте использовать схему интеграции по умолчанию для Splunk и Kaspersky CyberTrace Service.

Устранение неполадок ArcSight

В этом разделе приведена информация, с помощью которой можно решить проблемы, которые могут возникнуть при использовании Kaspersky CyberTrace с ArcSight.

Проблема: ArcSight не отображает события из Kaspersky CyberTrace Service или отображает их неправильно

Чтобы решить эту проблему, попробуйте выполнить следующие действия:

- Убедитесь, что сервер с Kaspersky CyberTrace Service включен и Kaspersky CyberTrace Service работает (для Windows-версии см. раздел Управление Kaspersky CyberTrace Service с помощью скрипта (Windows)).
- Убедитесь, что сервер ArcSight доступен с сервера Kaspersky CyberTrace Service.
- Убедитесь, что порт, указанный в строке подключения для вывода, открыт.
- Убедитесь, что ArcSight Forwarding Connector и ArcSight SmartConnector (для версии Windows, см. раздел Установка ArcSight SmartConnector (Windows)) запущены.
- Убедитесь, что Kaspersky CyberTrace Service прослушивает порт, на который Forwarding Connector отправляет данные из ArcSight ESM.
- Убедитесь, что Kaspersky CyberTrace Service отправляет события в ArcSight SmartConnector.

- Убедитесь, что ArcSight SmartConnector настроен правильно.

  Для этого выполните следующую команду:

  - `%ARCSIGHT_HOME%/current/bin/runagentsetup.sh` (в Linux)
  - `%ARCSIGHT_HOME%\current\bin\runagentsetup.bat` (в Windows)

  Здесь `%ARCSIGHT_HOME%` – это каталог, в котором установлен ArcSight SmartConnector.

Проблема: в активном канале не отображаются события после импорта нового пакета ARB

Чтобы решить эту проблему, попробуйте выполнить следующие действия:

Проверьте фильтр, используемый в активном канале:

1. Перейдите в раздел **Filters** → **Shared** → **All Filters** → **Public** → **Kaspersky CyberTrace Connector**.
2. Убедитесь, что в поле `device product` указано `Kaspersky CyberTrace for ArcSight`.

Создайте новый активный канал:

1. Удалите текущий активный канал и создайте новый.
2. Настройте новый активный канал следующим образом:
   - Установите параметры `Start Time` и `End Time` по своему усмотрению.
   - Установите для параметра `Use as Timestamp` значение `Manager Receipt Time`.
   - Если активный канал должен обновляться автоматически, выберите **Continuously evaluate** в разделе **Time Parameters** свойств активного канала.
   - В разделе **Filters** укажите фильтр, имя которого совпадает с именем самого активного канала. Доступные фильтры расположены в дереве ArcSight Console в разделе **Filters** → **Shared** → **All Filters** → **Public** → **Kaspersky CyberTrace Connector**, когда в раскрывающемся списке выбран пункт **Filters**.
   - В разделе **Fields** укажите элемент, имя которого совпадает с именем самого активного канала.

     Доступные поля расположены в дереве ArcSight Console в разделе **Field Sets** → **Shared** → **All Field Sets** → **Public** → **Kaspersky CyberTrace Connector**, когда в раскрывающемся списке выбран пункт **Field Sets**.

Проблема: Kaspersky CyberTrace Service не получает события из ArcSight

Чтобы решить эту проблему, попробуйте выполнить следующие действия:

- Убедитесь, что сервер с Kaspersky CyberTrace Service включен и Kaspersky CyberTrace Service работает (для Windows см. раздел Управление Kaspersky CyberTrace Service с помощью скрипта (Windows)).
- Убедитесь, что сервер ArcSight включен и ArcSight запущен.
- Убедитесь, что сервер Kaspersky CyberTrace Service доступен с сервера ArcSight.

  Для этого можно использовать утилиту `ping`.
- Убедитесь, что порт, указанный во входной строке подключения, открыт на сервере Kaspersky CyberTrace Service.

  Для этого можно использовать утилиту `netcat`.
- Проверьте регулярные выражения в конфигурационном файле Kaspersky CyberTrace Service или на вкладке **Параметры → Служебные оповещения** в веб-интерфейсе Kaspersky CyberTrace.
- Убедитесь, что установленный ArcSight Forwarding Connector работает.

  В Linux для этого можно использовать следующую команду:

  ```
  ps -Af | grep %DIR_NAME%/current/bin
  ```

  Здесь `%DIR_NAME%` – это каталог, в котором установлен Forwarding Connector. Если процесс Forwarding Connector запущен, информация о нем отображается в консоли.
- Если Kaspersky CyberTrace Service перестала получать события от ArcSight после импорта нового пакета ARB, зарегистрируйте ArcSight Forwarding Connector еще раз. Для этого выполните следующую команду и следуйте указаниям мастера:

  ```
  %ConnectorInstallDir%/current/bin/runagentsetup.sh
  ```

  Здесь `%ConnectorInstallDir%` – это каталог, в котором установлен ArcSight Forwarding Connector.

Проблема: ошибка аутентификации в ArcSight Forwarding Connector или учетная запись, предназначенная для использования в ArcSight Forwarding Connector, отсутствует

Чтобы решить эту проблему, попробуйте выполнить следующие действия:

1. Запустите ArcSight Console.
2. Выберите **Users** → **Shared** → **Custom User Groups**.
3. Создайте группу **Kaspersky CyberTrace Connector**.
4. Щелкните правой кнопкой мыши группу **Kaspersky CyberTrace Connector** и выберите **Edit Access Control**.
5. Выберите вкладку **Events**.
6. Нажмите на кнопку **Add**.

7. Выберите фильтр **CyberTrace forwarding events**.

8. Нажмите на кнопку **Save**.

9. В группе **Kaspersky CyberTrace Connector** укажите следующие параметры для учетной записи:

   - Любое имя пользователя (например, `FwdCyberTrace`)
   - В поле **type** укажите тип `Forwarding Connector`
   - Password

Эти учетные данные будут использоваться для пересылки событий из ArcSight в Kaspersky CyberTrace.

Устранение неполадок QRadar

В этом разделе приведена информация, с помощью которой можно решить проблемы, которые могут возникнуть при использовании Kaspersky CyberTrace с QRadar.

Проблема: QRadar не отображает события из Kaspersky CyberTrace Service или отображает их неправильно

Чтобы решить эту проблему, попробуйте выполнить следующие действия:

- Убедитесь, что сервер Kaspersky CyberTrace Service включен и Kaspersky CyberTrace Service работает.
- Убедитесь, что конфигурационный файл Kaspersky CyberTrace Service содержит правильную строку подключения для вывода, а формат выходных событий соответствует стандарту QRadar LEEF.
- Убедитесь, что Kaspersky CyberTrace Service добавлен в QRadar в качестве источника журналов.
- Убедитесь, что QID событий Kaspersky CyberTrace Service импортированы в QRadar.
- Убедитесь, что QID правильно сопоставляются с событиями Kaspersky CyberTrace Service.
- Убедитесь, что сервер QRadar доступен с сервера Kaspersky CyberTrace Service.
- Убедитесь, что порт, указанный в строке подключения для вывода, открыт.

Проблема: Kaspersky CyberTrace Service не получает события из QRadar

Чтобы решить эту проблему, попробуйте выполнить следующие действия:

- Убедитесь, что события пересылаются из QRadar в Kaspersky CyberTrace Service и правила маршрутизации заданы правильно.
- Убедитесь, что сервер Kaspersky CyberTrace Service включен и Kaspersky CyberTrace Service работает.

- Убедитесь, что сервер QRadar включен и QRadar запущен.
- Убедитесь, что сервер Kaspersky CyberTrace Service доступен с сервера QRadar.

  Для этого можно использовать утилиту `ping`.
- Убедитесь, что порт, указанный во входной строке подключения, открыт на сервере Kaspersky CyberTrace Service.

  Для этого можно использовать утилиту `netcat`.
- Проверьте регулярные выражения в конфигурационном файле Kaspersky CyberTrace Service или на вкладке **Параметры → Служебные оповещения** в веб-интерфейсе Kaspersky CyberTrace.

Проблема: после установки Kaspersky CyberTrace App for QRadar и добавления пользовательских свойств событий некоторые из этих свойств событий некорректно извлекаются из контекста события обнаруженной киберугрозы

Чтобы решить эту проблему, попробуйте выполнить следующие действия:

1. В QRadar Console выполните **Admin** → **Custom Event Properties**.
2. Чтобы найти пользовательские свойства событий со значением **Kaspersky CyberTrace** для параметра **Source Type**, отсортируйте таблицу по типу источника журнала.
3. Выберите строку, соответствующую неверно извлекаемому свойству, и нажмите кнопку **Edit**.

   Откроется окно **Custom Event Property Definition**.
4. В форме **Test Field** вставьте пример события, сгенерированного Kaspersky CyberTrace, которое содержит неверно извлеченное свойство.
5. На панели **Property Expression Definition**, в разделе **Extraction** измените значение в поле **RegEx** с `%property%=([^=]*)(?:\s[^=]+=)` на `%property%=\[(.*)\]`, где `%property%` — имя свойства.
6. Нажмите **Test**, чтобы убедиться, что требуемая часть события выделена в форме **Test Field**.
7. Нажмите на кнопку **Save**, чтобы применить изменения.

Проблема: после установки Kaspersky CyberTrace App for QRadar диаграмма не отображается

Чтобы решить эту проблему, попробуйте выполнить следующие действия:

- Дождитесь, пока QRadar загрузит данные.

  Сделайте то же самое при изменении имени источника журнала в настройках Kaspersky Threat Feed App.

Проблема: невозможно выполнить поиск с помощью Kaspersky CyberTrace App for QRadar, либо самостоятельная диагностика Kaspersky CyberTrace App for QRadar проходит неуспешно.

Чтобы решить эту проблему, попробуйте выполнить следующие действия:

- Убедитесь, что указано правильное значение настройки `Kaspersky CyberTrace Service Connection String` в Kaspersky Threat Feed App.
- Если Kaspersky CyberTrace установлен на сервере QRadar, добавьте необходимые правила iptables, как описано в разделе Configuring Kaspersky Threat Feed App.

Проблема: при добавлении нового регулярного выражения в формат выходных событий QRadar извлекает неверное соответствующее значение из событий обнаруженных киберугроз Kaspersky CyberTrace.

Чтобы решить эту проблему, убедитесь, что поля событий в строке разделены символом табуляции, как того требует стандарт LEEF.

Устранение неполадок RSA NetWitness

В этом разделе перечислены действия, которые можно предпринять, и проблемы, с которыми можно столкнуться при интеграции Kaspersky CyberTrace с RSA NetWitness.

Проверка поступления событий из RSA NetWitness в Kaspersky CyberTrace Service

Существует несколько способов проверить, отправляет ли RSA NetWitness события в Kaspersky CyberTrace Service:

- Можно проверить, есть ли в файлах журнала Kaspersky CyberTrace Service сообщения о поступлении событий из RSA NetWitness.

  В этом случае конфигурационный файл журнала Kaspersky CyberTrace Service (`bin/kl_feed_service_log.conf`) должен содержать строку `dbg` в элементе `WriteLog`.

- Можно воспользоваться утилитой netcat для отправки событий с сервера, на котором установлен RSA NetWitness, а затем проверить, добавлены ли соответствующие сообщения в файлы журнала Kaspersky CyberTrace Service.

- Можно остановить Kaspersky CyberTrace Service и использовать утилиту netcat для прослушивания событий от RSA NetWitness, для этого необходимо выполнить следующую команду:

  ```
  nc -l -p [port] -s [IP]
  ```

  Здесь `[IP]` и `[port]` — это IP-адрес и порт, на которые RSA NetWitness отправляет события для Kaspersky CyberTrace Service.

- Можно использовать утилиту tcpdump для прослушивания порта, на который должны приходить события из RSA NetWitness.

  Утилита tcpdump будет прослушивать порт `[port]`, если запустить эту утилиту с помощью следующей команды:

  ```
  tcpdump -neX port [port]
  ```

  Обратите внимание, что утилита tcpdump может использовать другой флаг (не `-neX`) в зависимости от операционной системы, в которой она запускается.

Если событие из RSA NetWitness не приходит, проверьте следующее:

- Проверьте правильность выполнения всех шагов, перечисленных в разделе Пересылка событий из RSA NetWitness.

- Проверьте, поступают ли события в RSA NetWitness от исходного устройства.

  Это можно проверить таким же образом, как проверяется, отправка событий из RSA NetWitness в Kaspersky CyberTrace Service.

- Убедитесь, что сервер, на котором установлен Kaspersky CyberTrace Service, доступен с сервера, на котором установлен RSA NetWitness.

  Это можно проверить с помощью утилиты ping.

Проверка сопоставления событий в Kaspersky CyberTrace Service с потоками данных об угрозах Kaspersky Threat Data Feeds

Обратитесь к файлам журнала Kaspersky CyberTrace Service, чтобы проверить, совпадают ли поля URL, хешей и IP-адресов событий с потоками данных об угрозах Kaspersky Threat Data Feeds. Файлы журнала должны содержать сообщения, похожие на сообщения, приведенные в следующем примере.

```
2016/07/25 20:16:30.162 DBG 0x7f99a6999700 UrlMatchingEngine. Normalized url: http://dbotnet.com/get.php?id=2&p=4

2016/07/25 20:16:30.162 DBG 0x7f99a6999700 FeedMatcher. http://dbotnet.com/get.php?id=2&p=4' is not detected for
RE_URL 'Botnet_CnC_URL_Data_Feed.json'

2016/07/25 20:16:30.164 DBG 0x7f99a799b700 UrlMatchingEngine. Normalized url:
http://botnet_domain_19.botnet_domain.com

2016/07/25 20:16:30.164 INF 0x7f99a799b700 FeedMatcher. Detect http://botnet_domain_19.botnet_domain.com' for
RE_URL 'Botnet_CnC_URL_Data_Feed.json'

2016/07/25 20:16:30.164 INF 0x7f99a799b700 Category: KL_BotnetCnC_URL
```

Если в файлах журнала отсутствуют подобные сообщения, проверьте, правильные ли регулярные выражения указаны в конфигурационном файле Kaspersky CyberTrace Service. Используемые регулярные выражения также можно проверить с помощью веб-интерфейса Kaspersky CyberTrace.

Проверка отправки событий из Kaspersky CyberTrace Service в RSA NetWitness

Проверить, отправляет ли Kaspersky CyberTrace Service события в RSA NetWitness можно следующими способами:

- Путем просмотра файлов журнала Kaspersky CyberTrace Service.

  Ниже приведен пример сообщений, записываемых в журнал при успешной отправке события в RSA NetWitness.

```
2020/05/20 17:09:12.987 INF 26341 siem New notification: KL_ALERT_UpdatedFeed --- parameters: [ 'feed':
'Blocklist.de_BlockIP.json', 'records': '35187' ]

2020/05/20 17:09:12.987 INF 26341 siem New notification: KL_ALERT_UpdatedFeed --- parameters: [ 'feed':
'Blocklist.de_BlockIP.json', 'records': '35187' ]

2020/05/20 17:09:12.987 DBG 26341 siem Connecting to '127.0.0.1:9998'

2020/05/20 17:09:12.987 DBG 26341 siem Sending notification KL_ALERT_UpdatedFeed

2020/05/20 17:09:12.987 DBG 26341 siem Notification KL_ALERT_UpdatedFeed has been sent successfully
```

Ниже приведен пример сообщения, записываемого в журнал, когда событие не может быть отправлено в RSA NetWitness.

```
2020/05/20 17:09:12.987 DBG 26341 siem Failed to send notification KL_ALERT_FailedToUpdateFeed (error: 0x80000072
(Unknown exception))
```

- С помощью утилиты tcpdump на сервере, который принимает события от Kaspersky CyberTrace Service.

  Утилита tcpdump прослушивает IP-адрес `[IP]` и порт `514`, если запустить эту утилиту с помощью следующей команды:

  ```
  tcpdump -neX src [IP] and port 514
  ```

  В этой команде следует указать IP-адрес, с которого Kaspersky CyberTrace Service отправляет события.

  Обратите внимание, что утилита tcpdump может использовать другой флаг (не `-neX`) в зависимости от операционной системы, в которой она запускается.

Если Kaspersky CyberTrace Service не отправляет события, проверьте следующее:

- Убедитесь, что файлы журнала Kaspersky CyberTrace Service содержат сообщения об обнаружениях URL, хешей или IP-адресов.

  Если таких сообщений нет, см. информацию в подразделе «Проверка сопоставления событий в Kaspersky CyberTrace Service с потоками данных об угрозах Kaspersky Threat Data Feeds». Также возможно, что в потоках данных об угрозах отсутствуют проверяемые URL, хеши и IP-адреса.

- Убедитесь, что в конфигурационном файле Kaspersky CyberTrace Service указаны правильные IP-адрес и порт назначения.

Проблема: RSA NetWitness не отображает события из Kaspersky CyberTrace Service

Если RSA NetWitness не отображает никакие события из Kaspersky CyberTrace Service, проверьте, правильно ли выполнена процедура в разделе Шаг 2. Отправка событий из Kaspersky CyberTrace Service в RSA NetWitness.

Обратите внимание, что RSA NetWitness может отображать события с устройства с задержкой в 10 минут.

Проблема: конфигуратор отображает сообщение об ошибке, если в параметре OutputSettings > ConnectionString указаны IP-адрес и порт Log Decoder.

Может отображаться сообщение об ошибке следующего вида:

```
Can't connect using the specified string. Press [Enter] to specify another string, or
type "ok" to continue with 10.10.0.127:514
```

Убедитесь, что сервер, на котором установлен RSA NetWitness, доступен с сервера, на котором установлен Kaspersky CyberTrace Service (например, с помощью утилиты ping).

Проблема: некоторые поля событий из Kaspersky CyberTrace Service не отображаются в метаполях в RSA NetWitness.

Если некоторые поля событий из Kaspersky CyberTrace Service не отображаются в метаполях в RSA NetWitness, выполните следующие действия:

- Убедитесь, что у метаполей, упомянутых в конфигурационном файле v20_cybertracemsg.xml, для параметра `flags` задано значение `None` в конфигурационном файле `/etc/netwitness/ng/envision/etc/table-map-custom.xml`.

  Если эти поля отсутствуют в файле table-map-custom.xml, добавьте их следующим образом:

  ```
  <mapping envisionName="url" nwName="url" flags="None" format="Text"
  envisionDisplayName="URL"/>
  ```

- Проверьте, все ли поля, описанные в разделе Пересылка событий из RSA NetWitness, содержатся в следующих конфигурационных файлах:

  - index-logdecoder-custom.xml (если не используется Concentrator)
  - index-concentrator-custom.xml

  Содержимое этих файлов можно просмотреть путем выбора **Administration** → **Services**. Затем выберите Concentrator (или Log Decoder), нажмите кнопку **Settings** () и выберите **View** → **Config** → **Files**. Отображается раскрывающийся список, содержащий все эти файлы.

  После редактирования файлов перезапустите Log Decoder или Concentrator, чтобы новые настройки вступили в силу.

  > Обновлять конфигурационный файл Concentrator (index-concentrator-custom.xml) следует только в том случае, если используются и Log Decoder, и Concentrator; Concentrator получает данные от Log Decoder, а Log Decoder получает события от Kaspersky CyberTrace Service. Кроме того, можно оставить без изменений конфигурационный файл Log Decoder (index-logdecoder-custom.xml), если Log Decoder не используется в качестве источника данных, в котором выполняется поиск событий, или если Log Decoder не используется для создания отчетов или информационных панелей.

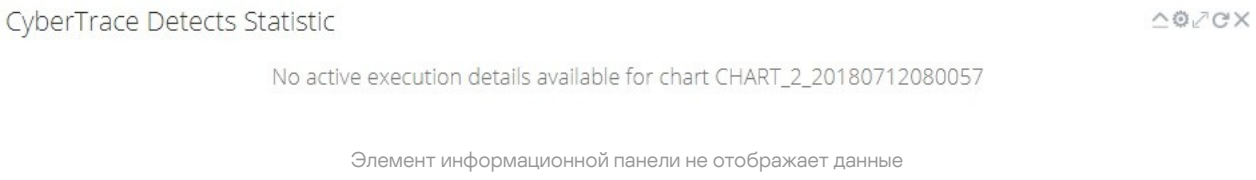
Если конфигурационные файлы не содержат необходимых полей, добавьте эти поля, как описано на в документации: https://community.rsa.com/docs/DOC-41760. Например, файл index-concentrator-custom.xml должен содержать следующие строки:

```
<key description="virusName" format="Text" level="IndexValues" name="virusname"
defaultAction="Open" />
<key description="user.src" format="Text" level="IndexValues" name="user.src"
defaultAction="Open" />
<key description="ip.src" format="IPv4" level="IndexValues" name="ip.src"
defaultAction="Open"/>
<key description="action" format="Text" level="IndexValues" name="action"
defaultAction="Open" />
<key description="msg" format="Text" level="IndexKeys" name="msg"
defaultAction="Open" />
<key description="event.source" format="Text" level="IndexValues" name="event.source"
defaultAction="Open" />
<key description="device.ip" format="IPv4" level="IndexValues" name="ip.dst"
defaultAction="Open"/>
<key description="ip.dst" format="IPv4" level="IndexValues" name="ip.dst"
defaultAction="Open"/>
<key description="url" format="Text" level="IndexValues" name="url"
defaultAction="Open"/>
<key description="checksum" format="Text" level="IndexValues" name="checksum"
defaultAction="Open"/>
```

Убедитесь, что значения полей `name` и `format` в конфигурационных файлах совпадают со значениями полей `nwName` и `format` соответственно в конфигурационном файле table-map-custom.xml.

Проблема: после импорта информационной панели Kaspersky CyberTrace не отображаются данные

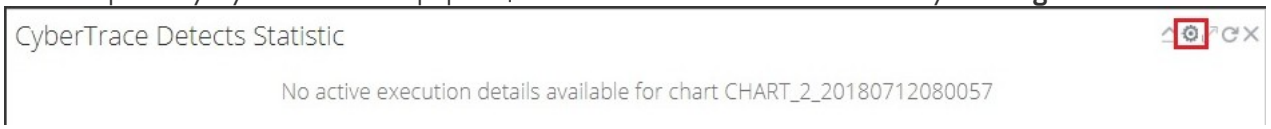
Вместо этого элемент информационной панели отображает сообщение об ошибке.



Элемент информационной панели не отображает данные

Чтобы исправить эту ошибку, настройте элемент информационной панели следующим образом:

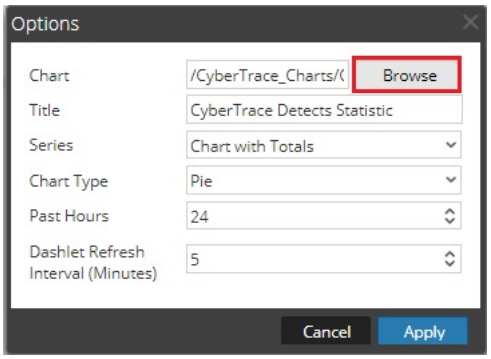
1. В правом верхнем углу элемента информационной панели нажмите на кнопку **Settings**.



Кнопка **Settings**

Откроется окно **Options**.

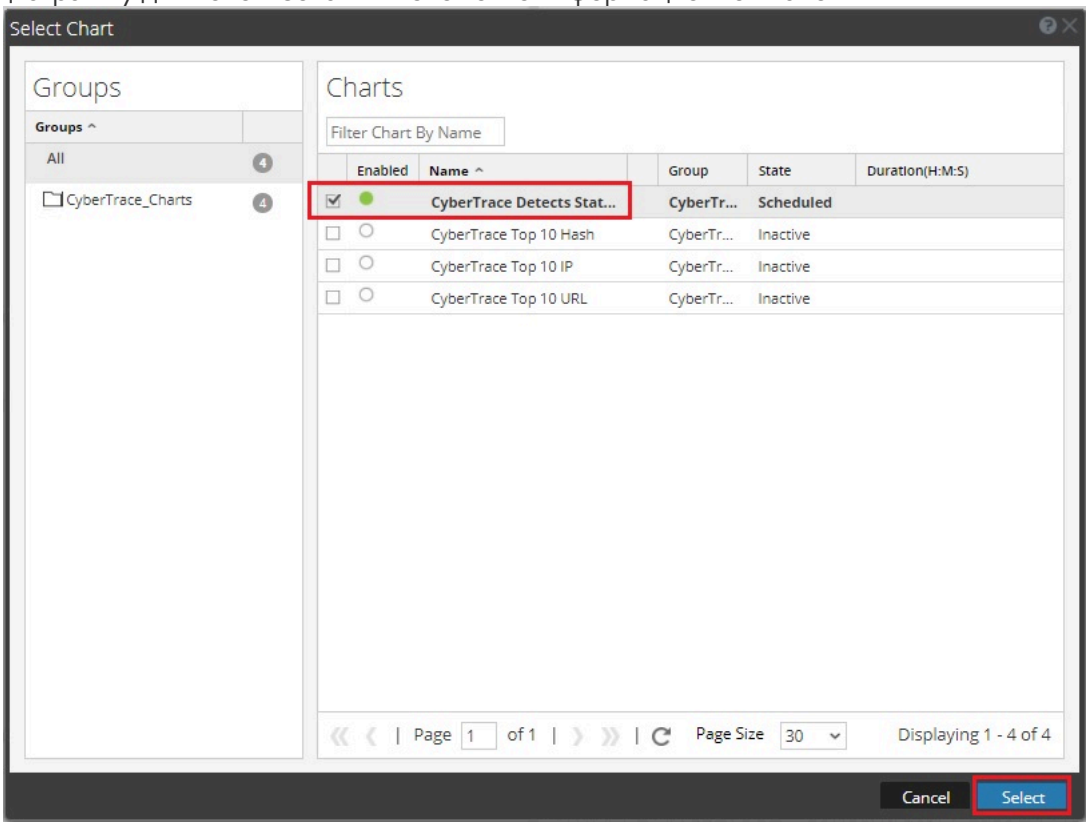
2. Нажмите на кнопку **Browse**.



Параметры элемента информационной панели

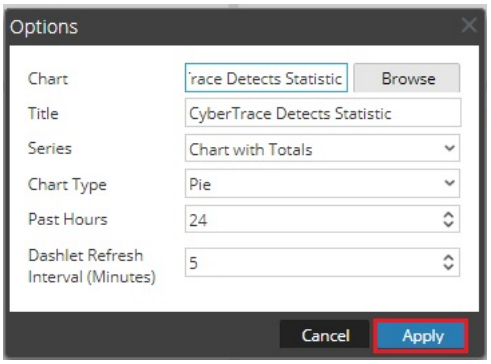
Откроется окно **Select Chart**.

3. Выберите диаграмму для использования в элементе информационной панели.



Выбор диаграммы

4. Нажмите на кнопку **Apply**.



Кнопка **Apply**

Проблема: Feed Utility отображает сообщение об ошибке «peer certificate cannot be authenticated with given CA certificates»

Не удалось выполнить аутентификацию сертификата. Убедитесь, что в системе установлены корневые сертификаты. Если корневые сертификаты не установлены, установите их по стандартной процедуре установки корневых сертификатов в используемой операционной системе.

Рекомендации по снижению рисков безопасности

При использовании Kaspersky CyberTrace рекомендуется принять следующие меры по снижению рисков безопасности:

- Ограничить доступ к серверу, на котором установлена Kaspersky CyberTrace.

  Это затруднит выполнение атак типа «отказ в обслуживании» (DoS) на этом сервере. Например, можно разрешить этому серверу обмениваться данными только с сервером администратора, с сервером, отправляющим события для проверки в Kaspersky CyberTrace Service, и сервером, который получает результаты проверки.

- Использовать решения сетевой безопасности.

  Если сеть скомпрометирована, злоумышленники могут перенастроить Kaspersky CyberTrace Service так, чтобы результаты проверки отправлялись на другой сервер.

- Если сервер, на который должны отправляться результаты проверки, не получал никаких событий в течение последних 24 часов, проверьте, не была ли настройка Kaspersky CyberTrace Service изменена злоумышленником.

Обращение в Службу технической поддержки

Если найти решение проблемы в документации Kaspersky CyberTrace не удается, обратитесь в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на все вопросы об установке и использовании Kaspersky CyberTrace.

«Лаборатория Касперского» предоставляет поддержку Kaspersky CyberTrace в течение всего жизненного цикла (см. страницу жизненного цикла продукта). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

Чтобы связаться со Службой технической поддержки, используйте контактную информацию, предоставленную вам при покупке лицензии Kaspersky CyberTrace.

Информация о стороннем коде

Информация о стороннем коде содержится в файле с именем legal_notices.txt, расположенном в подкаталоге `doc` каталога установки приложения.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Apache является либо зарегистрированным товарным знаком, либо товарным знаком Apache Software Foundation в Соединенных Штатах и/или других странах.

Apple, iPhone, macOS и Safari — товарные знаки Apple Inc.

LTS и Ubuntu — зарегистрированные товарные знаки компании Canonical Ltd.

Check Point — товарный знак или зарегистрированный товарный знак компании Check Point Software Technologies Ltd. или ее аффилированных компаний.

Cisco, Cisco IronPort, Snort, Sourcefire — зарегистрированные товарные знаки или товарные знаки компании Cisco Systems, Inc. и (или) ее аффилированных компаний в Соединенных Штатах Америки и ряде других стран.

Docker и логотип Docker — товарные знаки или зарегистрированные товарные знаки компании Docker, Inc. в Соединенных Штатах Америки и (или) других странах. Docker, Inc. и другие стороны также могут обладать правами на товарный знак в других терминах, используемых в данном документе.

Elasticsearch, Kibana и Logstash — товарные знаки Elasticsearch BV, зарегистрированные в США и других странах.

F5 — товарный знак F5 Networks, Inc. в США и ряде других стран.

Websense — товарный знак или зарегистрированный товарный знак Forcepoint в США и других странах.

Fortinet, FortiGate, FortiOS и FortiSIEM — зарегистрированные товарные знаки или товарные знаки Fortinet, Inc. в Соединенных Штатах Америки и (или) в других странах.

Google, Android, Chrome и Google Chrome — товарные знаки Google LLC.

IBM, ibm.com, QRadar — товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Juniper Networks и JUNOS — товарные знаки или зарегистрированные товарные знаки Juniper Networks, Inc. в США и других странах.

Linux — зарегистрированный товарный знак Линуса Торвальдса в США и других странах.

McAfee — товарный знак или зарегистрированный товарный знак компании McAfee LLC или ее дочерних компаний в Соединенных Штатах Америки и других странах.

Microsoft, Active Directory, Internet Explorer, Microsoft Edge, Win32, Windows и Windows Server — товарные знаки группы компаний Microsoft.

Mozilla и Firefox — товарные знаки Mozilla Foundation в США и других странах.

OpenSSL — товарный знак, принадлежащий OpenSSL Software Foundation.

Java, JavaScript и Oracle — зарегистрированные товарные знаки компании Oracle и/или аффилированных компаний.

Python — товарный знак или зарегистрированный товарный знак Python Software Foundation.

Red Hat и Red Hat Enterprise Linux — товарные знаки или зарегистрированные товарные знаки Red Hat, Inc. или ее дочерних компаний в США и других странах.

Debian — зарегистрированный товарный знак компании Software in the Public Interest, Inc.

Splunk — товарный знак и зарегистрированный товарный знак Splunk, Inc. в США и других странах.

Blue Coat, ProxySG и Symantec — товарные знаки или зарегистрированные товарные знаки Symantec Corporation или ее аффилированных компаний в США и других странах.

Rocky Linux — товарный знак Rocky Enterprise Software Foundation.

Trend Micro — товарный знак или зарегистрированный товарный знак компании Trend Micro Incorporated.

Названия, изображения и логотипы, связанные с продуктами и услугами компании UserGate, являются собственностью компании UserGate и/или ее дочерних или аффилированных компаний, а сами продукты являются собственностью UserGate.

Carbon Black — товарный знак или зарегистрированный товарный знак VMware, Inc. в США и других странах.

UNIX — товарный знак, зарегистрированный в США и других странах, лицензируемый исключительно компанией X/Open Company Limited.